ケーススタディ：IBMがQRadar ネットワークインサイトの性能を2倍に強化

業界における難題

コミュニケーションネットワークはこの数十年でとてつもない進化を続けています。クラウドの出現、5G携帯電話、そしてIoTは企業、ユーザ、アプリケーションによるコミュニケーションのあり方を変化させて来ました。倍増するデータ、拡大する帯域幅、より多くの端末、そしてボーダレスな企業の組み合わせは、装置やマネジメントコストを増やすことなく、より強固なセキュリティと法規制への対応を行うといった莫大なプレッシャーを生み出しました。

課題

IBMはサイバーセキュリティソリューション分野におけるグローバルリーダーとして認知されています。IBMのQRadarセキュリティ情報・イベントマネジメントシステム（SIEM）は、ネットワークとセキュリティのプロフェッショナルにとって望ましいソリューションです。エンドユーザが問題を早急に解明し対処する事を可能にするために、QRadar SIEMはリアルタイム、そして蓄積されたすべてのネットワークデータへの素早いアクセスを提供する必要があります。

業界の需要に対応するために、IBMはラインレートのネットワーク性能と全てのサイズにおけるパケットロスゼロの100%データキャプチャを含むクリティカルなアプリケーション要求を満たしながら、複数の側面においてQRadarを効率的に性能向上する必要がありました。また、深刻なラックスペース不足を考慮して、それらのソリューションの物理サイズを急激に拡張する事なく、パフォーマンスを最大化させる必要もありました。さらに言えば、複数のネットワーク装置間で最適化されたタイムスタンプ精度とセッションの一貫性を確保しつつ、それぞれの今後の性能向上を見越して、分析装置であるQRaderネットワークインサイト（QNI）の性能も向上する、といったオプションも必要でした。

ソリューション

IBMは製品の基本性能とキャプチャ要件を満たすべく、NapatechのSmartNICソフトウェア及びハードウェアを採用しています。NapatechのSmartNICは、複雑で負荷の高い様々なセキュリティ処理をホストCPUからオフロードすべく、高度に機能拡張されています。

性能を倍増

ラックスペース追加のコストを避けつつ、QNI装置のキャパシティを増強するために、IBMは2ソケット2Uサーバを採用しました。サーバ内部のトラフィック分配による浪費を回避してコンピュータリソースを最大限活用するため、先進的なNapatech SmartNICにソケットロードバランシング機能が追加拡張されました。

課題

IBMはQRadar SIEMを物理サイズやソリューションコストを急激に増加させることなく、その性能を最大限向上させる必要がありました。さらにパフォーマンスを増強させるため、多岐にわたる装置間でそのタイムスタンプ精度とセッションの一貫性を確保しつつ、QRadarネットワークインサイトを性能向上するオプションも必要でした。

ソリューション

IBMは複雑で負荷の高いセキュリティ処理をホストCPUからNapatech SmartNICにオフロードすることで、貴重なコンピュータリソースを最適化することができました。

利点

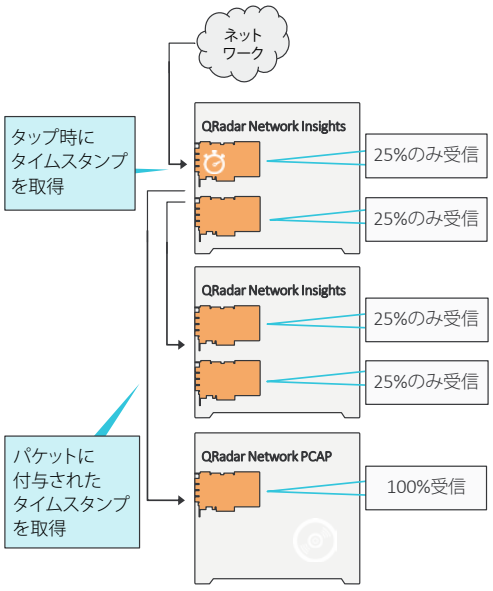
- 2倍のアプリケーション性能
- 実質的なコスト削減
- 装置間タイムスタンプの完全な一貫性
- ソフトウェアの変更は不要

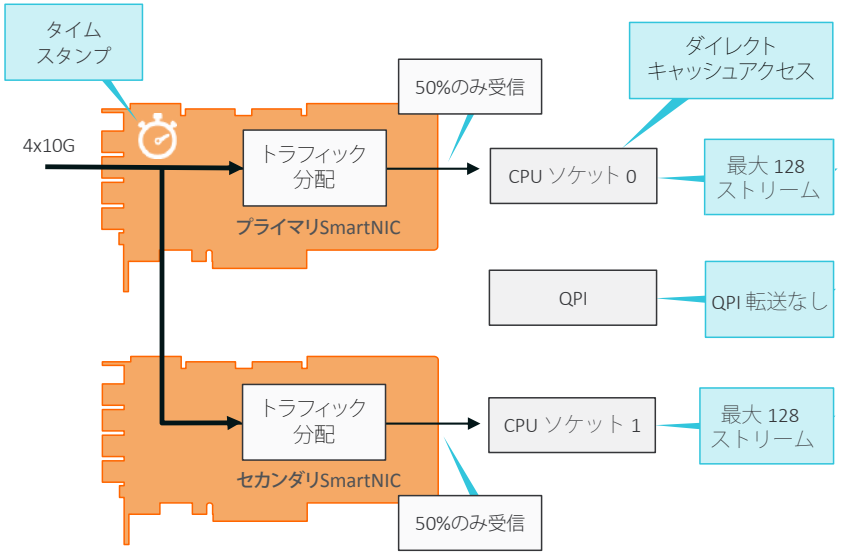
第一の目標は、この2ソケットサーバにおける2つのCPU間でトラフィックが効率的に分配されている事を保証する事でした。この分配をQuickPath Interconnect（QPI）に依存すると、性能が劣化し拡張性を損ないます。これを避けるため、ソケットロードバランシング機能はプライマリとセカンダリSmartNIC間でトラフィックを分配し、2つのCPUソケットそれぞれに専属的なパケットストリームを生成することでQPIをバイパスします。

完全なセッションの一貫性を保証するために、各パケットはプライマリSmartNICでナノ秒精度の正確なタイムスタンプが付与され、関連するセッション／フローごとに2つのCPU間でインテリジェントに分配されます。IBMはこれにより、QNIソフトウェアにまったく変更を行うことなく、2Uフォームファクタを維持しつつアプリケーションの性能を２倍にしました。

パフォーマンスの倍増

QNIソフトウェアに変更をかける事なく、さらなる大きなパフォーマンス増強を実現するために、ソケットロードバランシング機能と一点集中によるタイムスタンピングメカニズムが、複数のQNI装置にトラフィックを分配するために使用されました。また 、フォレンジック調査においてあらゆる事象が簡単に抽出できるよう全てのパケットをキャプチャし保存するため、このコンセプトはNapatechのcapture-to-diskテクノロジをベースにしたQRadarネットワークPCAP装置にも適用されています。





処理のため装置へのダウンストリームにパケットがフォワードされる前に、ネットワークタップポイントに接続されたQNIによってナノ秒精度の正確なタイムスタンプが付与されます。この同期性によって、素早くシームレスなデータ連携、および様々なQRadar装置間でユニークなセッションの認識が可能となり、迅速かつ正確なフォレンジック調査のために必要な一貫性を提供します。

利点

- 2倍のアプリケーション性能
- 実質的なコスト削減
- 装置間タイムスタンプの完全な一貫性
- ソフトウェアの変更は不要

さらにケーススタディを見る：
www.napatech.com/resources/case-studies

DN-1132 Rev. 1-JA

ヨーロッパ・中東・アフリカ
Napatech A/S
デンマーク コペンハーゲン

Tel. +45 4596 1500
info@napatech.com
www.napatech.com

北米
Napatech Inc.
マサチューセッツ州ボストン
カリフォルニア州ロスアルトス
ワシントンD.C.

Tel. +1 888 318 8288
info@napatech.com
www.napatech.com

アジア太平洋
Napatech China/South Asia
台湾 台北
Tel. +886 2 28164533 Ext. 319

ナパテックジャパン株式会社
日本 東京
Tel. +81 3 5326 3374
ntapacsales@napatech.com