ポスター
# ポスター1
# ネットワーク・ Web活用
2017年11月21日(火) 14:15 〜 15:15 L会場（ポスター会場1） (12F ホワイエ)

[2-L-1-PP1-2] 既存ネットワークにおけるネットワーク侵入防御システムの導入の検討

中村 直毅, 葭葉 純子, 伊藤 和哉, 長瀬 祥子, 中山 雅晴, 冨永 悌二 （東北大学医学系研究科）

世界各国においてウイルス感染の被害やサイバー攻撃が猛威を振るっている。東北大学病院(以後、本院とする)では、これらの被害や攻撃を最小限に食い止めるため、ネットワーク侵入防御システム（ IPS）を導入することにした。 IPSを適用するネットワークは、不特定多数のサイト向けの通信の監視が不要である診療、ゲノムネットワークに対象を限定し、シグネチャの細かなチューニングを避け、運用負荷を抑えた IPSの導入を想定している。本院のネットワークは、 Firewallの仮想化技術を用いた多段構成で Firewallを複数配置しているとともに、通信ログ取得およびウイルス・ URLフィルタを適用した多段のプロキシサーバを配置した構成となっている。本稿では、本院の現行のネットワークに対して、 IPSを適用するための概要と検証の取り組みについて報告する。
現行ネットワークでは、クライアントの HTTP通信は、多段のプロキシを介して行われており、クライアント・プロキシ間やプロキシ間の通信で監視しても IPSが正常に機能しない。そのため、 IPSでは、最上位のプロキシサーバにおける HTTP通信の監視が必要である。しかしながら、最上位のプロキシサーバにおける通信は、診療、ゲノムネットワークだけに留まらず、ネットワーク全体の HTTP通信を監視することになるため、研究用のネットワークも対象になり運用に支障が生じてしまう。そこで、診療、ゲノムネットワークのクライアント端末の設定にてプロキシ設定を解除して、プロキシされていない通信を IPSにて監査し、その後、 WCCP(Web Cache Communication Protocol)を用いて透過型プロキシとして設定されたプロキシサーバへ通信を振り向け、従来と同様に多段プロキシを介して HTTP通信するよう構成変更することにした。検証環境を構築し、 WCCPによる通信制御、 IPSによる通信の監査、単一機器に障害等が発生しても通信影響が無いことを確認し、本院のネットワークに導入可能であることを確認した。今後は、本検証に基づいて実環境に IPSを導入する予定である。

既存ネットワークにおけるネットワーク侵入防御システムの導入

中村 直毅[*1 *2]、葭葉 純子[*1]、伊藤 和哉[*1]、長瀬 祥子[*1]、
千葉 雅俊[*2]、田山 智幸[*2]、中山 雅晴[*2]、冨永 悌二[*1]
*1 東北大学医学系研究科情報基盤室、*2 東北大学病院メディカル IT センター

An Introduction of the Intrusion Prevention System in Present Network

Naoki Nakamura[*1 *2], Junko Yoshiba[*1], Kazuya Ito[*1], Sachiko Nagase[*1],
Masatoshi Chiba[*2], Tomoyuki Tayama[*2], Masaharu Nakayama[*2], Teiji Tominaga[*1]
*1 Information Infrastructure Office, Graduate School of Medicine, Tohoku University
*2 Medical IT Center, Tohoku University Hospital

Cyber attacks and computer virus infection are alarmingly high in recent years. As Network Intrusion Prevention System (IPS) is effective for both detection and preventing from these attacks or infections, authors in this paper introducing IPS into a large-scale network where 20,000 or more sets of terminals are connected. In present network, high-speed firewalls are already there. So we setup IPS equipment utilizing these existing firewalls. By examining, how to build IPS equipment in a gateway, we confirmed that it could be easily installed in present network using L2 bridge function. Then we considered the setup of both firewall and HTTP proxy servers in such a way, that the network where the client is connected can be identified by the source IP address of the traffic. Based on these ideas, we confirmed the normality of the system with experimental environment. We have also adjusted firewalls and proxy servers and installed IPS equipment in present network. Then we verified the built functions to carry out traffic surveillance in both IDS and IPS mode. Furthermore, we checked that the policy of IPS was correctly controllable according to the network where the client is connected. Now we are advancing optimization of the setup of equipment, verifying the function of IPS equipment.

Keywords: Security, Intrusion Detection System, Intrusion Prevention System

1. はじめに

世界各国でウイルス感染の被害やサイバー攻撃が猛威を振るっている。これらを阻止するためには、ネットワーク侵入防御システム(IPS)を導入することが効果的であると知られている。一方、IPS 装置を導入・運用するには、専門的な知識が要求され、シグネチャやルールの定期的なチューニングも必要であり、脅威を検出した際の対処に要する運用上の負荷についても考慮しながら進める必要がある。東北大学星陵キャンパスのネットワークは、東北大学病院、医学系研究科、歯学研究科、東北メディカル・メガバンク機構で共通のインフラで統合して運用管理しており、2 万台以上の端末が接続されている。今回、この大規模なネットワークに対して、IPS 装置を適用することになった。本稿では、本ネットワークへの IPS 装置の導入について報告する。

2 設計

2. 1. ネットワーク構成の概要

東北大学星陵キャンパスのネットワークは、Firewall の仮想化機能や L3 スイッチの VRF(Virtual Routing Forwarding)機能を積極的に活用し、図1のネットワーク論理構成図に示すように、教育・研究、診療支援システム、コホート研究、ゲノム解析システム、バイオバンクシステム、全県レベルの地域医療連携システム用の Firewall やルータを並列に配置して、適切に通信制御を行い、セキュリティレベルの異なるネットワークを運用している。本ネットワークでは、既に高速かつ高性能な Firewall を導入しており、既存の Firewall の利用を継続したまま、IPS 装置を新たに導入する。

2. 2. 監視対象

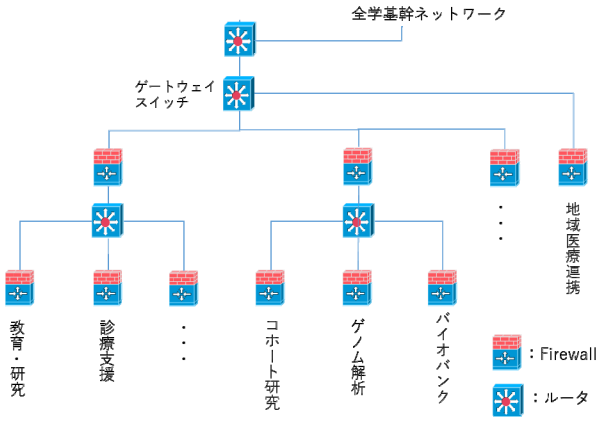


図１　星陵キャンパスのネットワークの概要

IPS 装置による通信の遮断を実施する対象は、不特定多数との通信が発生しない、診療支援システム、ゲノム解析システム、バイオバンクシステム、地域医療連携システムに限定する。これらのネットワークに対しては、安全を担保するためにトラフィックの遮断が必要と判断される通信を強制的に遮断することで、IPS 装置の運用に伴う稼働の軽減を図る。また、脅威の検出や遮断のルールやシグネチャのチューニングは、基本的には自動設定とし、運用開始後の調整は極力実施しない運用を想定している。一方、不特定多数との通信が多数を占める教育・研究用ネットワークでは、IPS 装置による通信の遮断は当面見送り、IDS 機能として動作させ、ネットワーク上の脅威を検出することを目的とする。IPS 装置による通信の遮断は試行運用を通して、徐々に適用することを想定している。

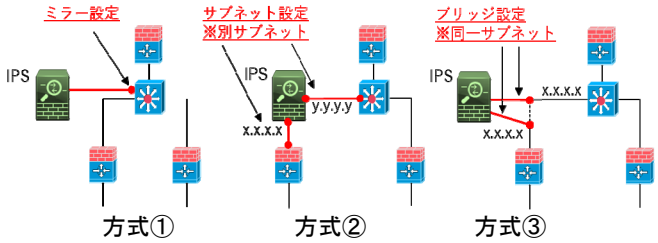


図 2 監視トラフィックの取得方式

2.3. 監視トラフィックの取得方式

IPS 装置を接続するには、図 2 に示すように、3つの方式が挙げられる。

① 監視したい通信のミラーポートを既設スイッチで設定し、スイッチから出力されるトラフィックを IPS 装置で監視する。この方式では、既存ネットワークへ簡単に組み込むことができ、通信の脅威を検出することが可能である。一方、危険な通信を遮断できないデメリットを有する。

② IPS 装置に IP アドレスを付与してルータとして動作させ、既存機器を含めてネットワーク論理構成を再設定し、監視したいトラフィックを IPS 装置にルーティングすることで通信を監視する。この方式では、ネットワークの論理構成の見直しが必要である。また、複数箇所で通信を監視するには、既存機器の設定に加えて、IPS 装置において複数のルーティングテーブルを処理できる仮想ルータ機能を備えている必要がある。

③ L2 のブリッジ機能を活用し、監視トラフィックが IPS 装置を経由するように設定し、現行のネットワークに透過的に組み込む。この方式では、IPS 装置において 2 つのインターフェースを作成し、監視ポイントのネットワークを論理的もしくは物理的に接続し、2 つのインターフェースをブリッジ接続して、監視対象のトラフィックが IPS 装置を経由するように制御するため、ネットワークの論理構成を維持したまま IPS 装置を組み込むことができる。

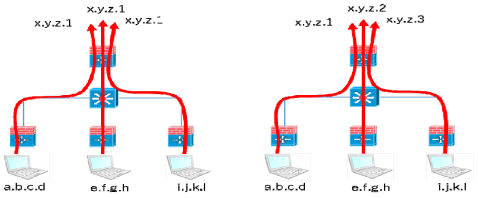
本稿では、IPS 装置を現行のネットワークに組み込む際の親和性を重視し、方式③によって監視トラフィックを取得する。

2.4. 監視ポイントの配置

IPS 装置によって脅威を監視する場合、クライアントを収容している Firewall や VRF の通信を監視する方法と、ゲートウェイを経由する対インターネット向けの通信を監視する方法が挙げられる。セキュリティレベルの異なるネットワークを細かく監視するためには、ネットワークにある全ての Firewall や VRF の通信を監視することが望ましい。しかしながら、ネットワークにある全ての Firewall や VRF を監視する場合、ネットワークの構成変更が発生する度に、IPS 装置やネットワーク機器の設定変更が必要となり、管理者の運用稼働が増大する懸念が生じる。そのため、ゲートウェイを経由する対インターネット向けの通信を IPS 装置の監視ポイントにする。

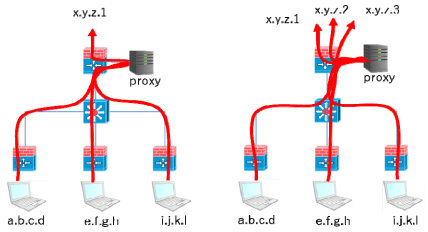
2.5. 既存機器の送信元 IP アドレスの見直し

今回対象としている星陵キャンパスにおけるゲートウェイの監視ポイントでは、セキュリティレベルが異なるネットワークに収容されているクライアントからのトラフィックが混在している。しかしながら、トラフィックの送信元 IP アドレスは、クライアントの IP アドレスではなく、下位の Firewall で NAT される IP アドレスとなっている場合がある。また、プロキシサーバを使っているクライアントがアクセスする HTTP トラフィックは、同じ IP アドレスのプロキシサーバを介して対インターネット通信をしている。そのため、ゲートウェイを通過するトラフィックの送信元 IP アドレスは同じアドレスになっており、IP アドレスを確認しても接続元のネットワークを判別することができない。そのため、クライアントを収容しているネットワークセグメント毎に応じて希望する処理を行うことができない。そこで、接続元ネットワークの送信元 IP アドレスを適宜調整する。具体的には、Firewall においては、図 3 に示すように、送信元のクライアントのネットワークセグメントで NAT される IP アドレスが収容元のネットワークに応じて異なるように設定を見直す。また、図 4 に示すように、プロキシサーバの送信元 IP アドレスを収容元のネットワークに応じて異なるように設定を見直す。加えて、HTTP 通信のヘッダの X-Forwarded-For 属性にクライアント IP のアドレスを付与するようにプロキシサーバを設定し、接続元のクライアントの IP アドレスを IPS 装置に通知することで効率的に処理できるように設定を見直す。



＜変更前＞ ＜変更後＞

図 3 Firewall の NAT 後の送信元 IP アドレス設定の概要



＜変更前＞ ＜変更後＞

図 4 Proxy サーバの送信元 IP アドレスの設定の概要

以上のように IPS 装置の監視ポイントをゲートウェイにおいて配置し、正常に監視できるようにする。

3. IPS 装置の検証と適用

図 1 と同様なネットワークの検証環境を構築し、実機を用いたシステムの正常性および切り替え手順の確認を実施した。さらに、ゲートウェイスイッチにおいてトラフィックのミラーポートを用意し、IPS 装置によりトラフィックを監視し、処理がオーバフローすることなく正常動作することを検証した。

次に、IPS 装置を既存ネットワークに接続し、Firewall およびプロキシサーバを再設定し、IDS モードによるトラフィックの監視ができることを確認した。また、クライアントが収容されているネットワークに従ってルールを定義し、適切に制御できることを確認した。IPS 機能については、検証用のネットワークにおいて基本機能を確認した所である。

4. まとめ

本稿では、東北大学星陵キャンパスにおける IPS 装置の導入の概要について述べた。現在は、IPS 装置の検証と導入が完了した。今後は、IPS 装置の設定調整を進めながら、設定の最適化を図るとともに、運用負荷が過度に課されない運用を実現するための検討を進める予定である。