[Work in Progress] 研究報告

次世代ファイアーウォール機器の評価検証について

中村 豊[1,a)]　佐藤 彰洋[1,b)]

Validation of next generation firewall products

本稿では平成 28 年度より開始した、UTM 機器の評価検証について述べる。国立大学法人では予算が削減されているにもかかわらず、情報セキュリティに関して高度な対応を要求されている。また、昨今の情報セキュリティインシデントでは愉快犯的な事故ではなく、事業継続に致命的な損害を与えるような事象も発生している。このような情報セキュリティインシデントに対処するために様々な機器がメーカーから提供されている。しかしながら、それらの機器が実際にどの程度の検出精度で動作するかは機器を導入しなと不明な場合がほとんどである。そこで本稿では、様々なメーカーが提供している評価機を試験運用し、実際の運用トラヒックを適用して UTM 機器がどの様な出力を出すのかについて検証を行った。

大学の置かれている前提条件として、1. 大学内はすでに何らかのマルウェアに感染している端末が複数存在する。2. 1. の理由により入口対策の実施はあまり効果的ではない。という事情が存在する。1. については学生個人の持込み PC が汚染された状態で持ち込まれているため、防止することができない。したがって大学側の対策としては、すでに感染している端末が存在していることを前提として、情報漏洩前の対策が重要となってくる。具体的には学内から学外へのマルウェアの C&C サーバへの通信の検出が重要であると思われる。また、マルウェアの種別の識別や、どのような通信が発生しているため感染が疑われているのか？のエビデンスが必要であると考える。

図 1 に評価を実施したネットワーク環境を示す。

本学では SINET5 との接続の境界に Fortinet 社の FG-1000C を導入して、外部からの攻撃トラヒックの遮断を実施している。評価機は FG-1000C を通過したポートを Juniper Networks 社の EX4550 でポートミラーしたトラヒックを検査する。

以下に UTM 評価における評価軸について述べる。本稿ではこれらの評価軸を基にして、様々なメーカーの UTM の動作について報告する。

[1] 九州工業大学 情報科学センター
Kyushu Institute of Technology, Information Science Center
1-1 Sensui-cho, Tobata-ku, Kitakyushu, 804–8550, Japan
[a)] yutaka-n@isc.kyutech.ac.jp
[b)] satoh@isc.kyutech.ac.jp

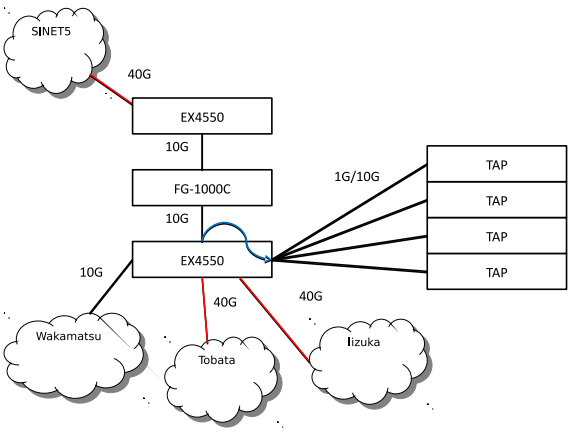

図 1　UTM 評価ネットワーク環境

(1) IPS
外部からサーバの脆弱性に対する攻撃や、brute force 攻撃の検出、また内部から外部への攻撃トラヒックの検出が要求される。

(2) AV/TP
外部から侵入してくるメールに添付するウィルスの除去、HTTP 通信における drive by download の検出、また外部から学内へのウィルスの注入などの検出や除去が要求される。

(3) Web filter
訪問サイトの分類や脅威の判定が要求される。

(4) Application control
利用されているアプリケーションの分類や流量の表示が要求される。

(5) C&C サーバへの通信検出
学内から学外への Botnet への通信や C&C サーバへの通信の検出が要求される。

(6) マルウェア検体のダウンロード可否
AV/TP や Sandbox 機能を用いたマルウェア検体の取得が可能かどうか？

(7) Sandbox の動作

(8) 仮想ドメインの有無

(9) ダッシュボードの動作

(10) TAP, one arm, sniffer モードの可否