2010 2nd International Conference on Education Technology and Computer (ICETC)

The Trends of Intrusion Prevention System Network

Deris Stiawan
Faculty of Computer Science,
Sriwijaya University, Indonesia.
Faculty of Computer Science &
Information System, Universiti
Teknologi Malaysia.
deris.stiawan@gmail.com

Abdul Hanan Abdullah
Faculty of Computer Science &
Information System, Universiti
Teknologi Malaysia.
hanan@utm.my

Mohd. Yazid Idris
Faculty of Computer Science &
Information System, Universiti
Teknologi Malaysia.
yazid@utm.my

***Abstract*— In recent years, Intrusion Prevention System (IPS) have been widely implemented to prevent from suspicious threat. Unlike traditional Intrusion Detection System, IPS has additional features to secure computer network system. The additional features identifying and recognizing suspicious threat trigger alarm, event notification, through responsible response. However, IPS has issues problem, which affect the utilized overall system.**

In this paper we present the main challenging problem and steps to avoid that, such as (i) accuracy signature, (ii) the traffic volume, (iii) topology design, (iv) quota usage logging, (v) protecting intrusion prevention system, (vii) monitoring sensor, and (viii) collaboration of UTM. Finally, as part of our enhancements, we explored the possibility of making framework to collaborate and integrated various technologies of defense system, we called Unified Threat Management (UTM).

Keywords - Issued challenge of Intrusion Prevention, Collaboration defense system, Unified Threat Management (UTM).

I. INTRODUCTION

Over the past few years, computer security has become a main issues, the increment number of trend and attack. The security issue can affect factor of the reliability (including performance and availability) in internetwork [14]. There is several vulnerability system to attempted attacks from the network, application or operating system. According to CSI/FBI survey [11], the company business has dollar amount of loss by type of attack. Meanwhile, to secure the system, the enterprise uses several technology security systems, and almost 69% of them use intrusion prevention to defense from threat and attack.

Intrusion prevention is a new approach system to defense networking systems, which combine the technique firewall with the Intrusion detection properly, which is proactive technique. Prevent the attacks from entering the network by examining various data record and prevention demeanor of pattern recognition sensor. When an attack is identified, intrusion prevention block and log the offending data. The primary IPS uses signature to identify activity in network traffic and host perform detection on inbound – outbound packets and would be to block that activity before the damage and access network resources.

Basically, to early prediction and prevention suspicious threat, there are two approaches, Host-based approach and Network-based approach [4],[7],[8],[10]. *First*, Host-based approach : Host-based is currently popular technology, it is check for suspicious activity from the host or operating system level, the monitoring location use the agent component, prevention earlier under level operating system, which is useful before the host reaching the target of attack. Provide intrusive this activity, unfortunately, which could produce numbers of alert and increase consumed of bandwidth, will affect performance computer utilize. Unfortunately, cannot examine traffic that doesn't allow. *Second,* Network-based approach: focus on network, sniffing and identifying packet all inbound-outbound in out of the network. The combining Network-based with other security component, provides an active comprehensive network security. Furthermore, the system does not require the system to be installed in every node.

The rest of this paper is structured as follow. In section 2, we describe analysis and identify main issues of challenge in IPS. In section 3, we describe the literature finding to shown our anticipation, and section 4 conclude the paper with of our results and a discussion of future work.

II. ANALYSIS & IDENTIFY

In this section, we proposed to describes a circumstance issues in IPS, as following :

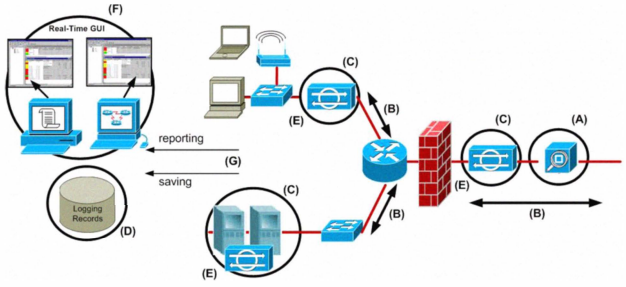

Figure 1. An example of topology to describe issues challenge of intrusion prevention, with number (A) accuracy signature, (B) the traffic volume, (C) topology design, (D) quota usage logging, (E) protected intrusion prevention, (F) monitoring sensor, (G) collaboration of UTM.

A. Signatures

A common issue prevention system is that difficult to identify and recognized analyzing packet in real-time traffic.

To detect suspicious threat, there are two approaches, Host-based and Network-based approach.

Signature is primary factor in intrusion prevention, identify to find something and stop it must be distinct characteristics. Signature triggers, using trigger action which can be applied atomic and stateful signature. There are three trigger mechanism, such as (i) pattern prevention, (ii) anomaly-based prevention, (iii) behavior-based prevention [1],[4],[5]. The past research on using technique method with wavelet [1], and [2] present the technique a Hidden Markov Model (HMM) to model sensor, [8] proposal the incremental-learning algorithm, [9] Present Pattern-matching algorithm, and [10] proposed the artificial immune algorithm.

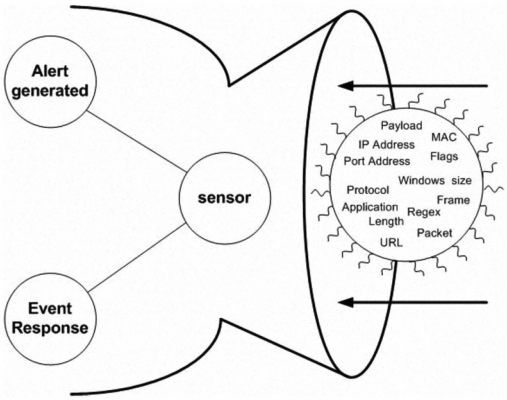

Figure 2. The sensor will trigger alert if identify and recognized suspicious threat, which is alert warning true or false alarm. Meanwhile, event response can do logging, block, allow, deny.

IPS has a sniff able to identify all inbound-outbound packet data. The placements of Host-based and Network-based devices affect the accurately of sensor. The sensor produce alert, which is to identify suspicious data and trigger alert if offending data, a signature needs the trigger to recognize:

1. Pattern-based Prevention : to identify a specific pattern, to represent a textual or binary string. Pattern prevention provide following mechanism, such as [4], [5] : (i) Pattern Detection (Regex) : a Regex is a pattern-matching language that enables to defines a flexible custom search string and pattern, (ii) Deobfuscation techniques [15] : focuses on obfuscating the concrete syntax of the program. The idea is to prevent an attacker from understanding the inner workings of a program by making the obfuscated program, An example of this is changing variable names or renaming different variables in different scopes to the same identifier
2. Anomaly-based Prevention : is also sometimes as profile-based prevention, we must build profiles that obviously defines what activity is considered normal activity, in figure 2, is a considered normal, then anything that deviates from this normal profile generates trigger alert [2],[12]
3. Behavior-based Prevention, is similar to pattern prevention, but trying to define specific patterns, the behavior define classes of activity that are know to be suspicious [1],[6].

The Alert Generated by the sensor, which in the situation trigger of alarm (valid and invalid but feasible) from sensor, there are four alert generating, such as (i) The true negative, which in normal user traffic and no alarm generated, (ii) true positive generate alarm after the attack traffic, (iii) false negative will be silent no alarm generated in attack traffic, meanwhile, (iv) the false positive produce alert to identify normal activity traffic , to reduce false positives alert is the main focus.

B. Traffic Volume

The second issues of IPS is traffic volume, which is affect in sensor using of, where, the increasing of the bandwidth traffic monitor will affect the overall utilizing performance. We need to verify actual amount of inbound-outbound traffic usage. In the figure 3, amount of traffic affect because of network segments (enterprise or service provider) and the number of the sensors placements, the amount of data which two interfaces fast Ethernet, will differ with four interfaces Gigabit Ethernet. This is due to real-time inbound-outbound traffic data.

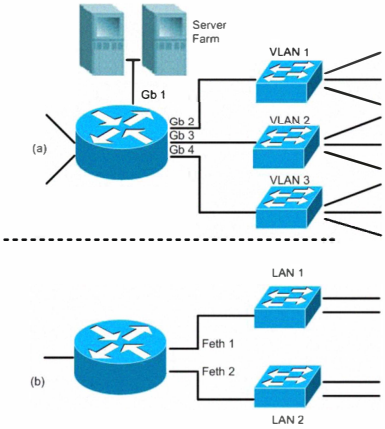

Figure 3. Example topology affect of traffic volume, (a) service provider, (b) enterprise.

The conjunction with main issue, the performance network will affect overall network utilization. This is important because any network node can suffer a variety of problems, including hardware faults. Report of error operating system, network devices produce broadcast and consumed bandwidth. Therefore, collisions will occur.

The number of source points for traffic which tunes from core server nodes to edge client nodes increases with the proportion of peer-to-peer traffic. We equalize the volume of download traffic across nodes, whether all traffic is client server web traffic or all traffic is peer-to-peer traffic [13].

C. Design Topology

In this issue, we will identify the access anywhere to conduct, furthermore, we provide permission to connecting business partner and remote telecommutes. The purpose define location, as following, *First*, Inside: the trusted side network monitoring, *Second*, Outside: the untrusted side network monitoring, however, the monitoring in outside will do inside and DMZ, and *Third*, DMZ : Demilitarization side, to identify and monitoring detect server farm area.

There are two factor that will be affect, *First*, the sensor placement, and *Second*, the number of sensor. The sensor, recognize and identify suspicious data and trigger alert if identify suspicious threat. Furthermore, the situation trigger of alarm (valid or invalid but feasible) from sensor to event response. Previous work introduced [7], the attempt to develop intrusion based on SNMP, unfortunately, SNMP based have problem that vulnerability MIB and agent.

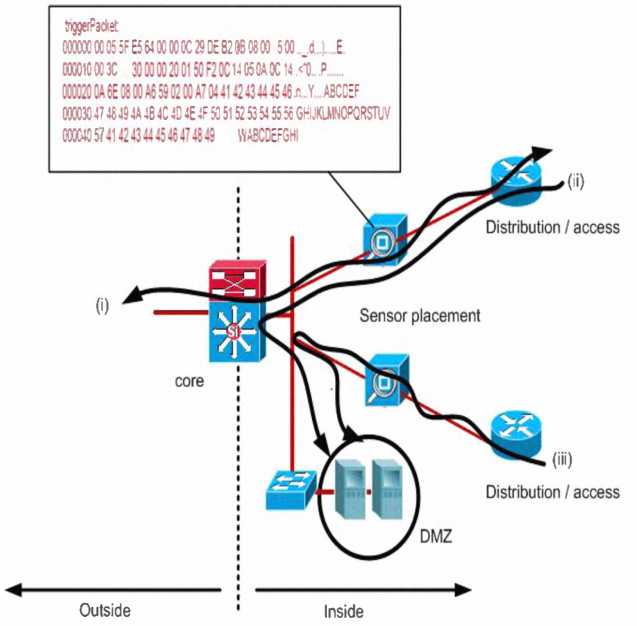

Figure 4. The penetration suspicious threat, such as (i) Attack from two sides, inside and outside (zombie, agent, scanning, shell inject, etc), (ii) attack which in attempt from inside to DMZ, and (iii) several user access to DMZ, to penetration and interrogation system, while zombie to flooding DMZ.

D. Logging

The past researcher [15], proposed all system logs that stored in secured environment. Modules redundancy allows high reliability. Databases configuration depends on signatures amount and average update time.

In this issue, we evaluate challenges quota usage, there are many log file produce from logging system, which conduce the large storages, logging data transaction, logging attacker traffic, logging victim traffic, logging incident record, logging incident notification, logging summary report, logging failure report, etc.

From Figure 5, the problem is the capacity of media storages to accommodate it. Nevertheless, replication, backup and elimination scheduling are a mechanism to efficiency and effective logging storages, which it the part of policy.

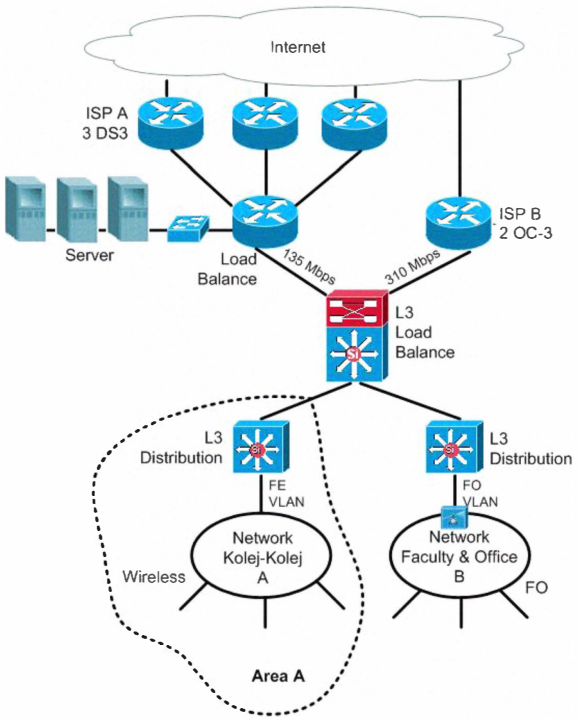

Figure 5. Topology observation, which in Area A, we have produce logging file 150 MB/s. The Intrusion Prevention system made produces large file/sensor, with increasing the number of sensors and traffic network. In Figure 5, represent the observation our network, which bandwidth real-time traffic 135 Mbps with ISP A (three backbone with load balance). The network area A, will produce 150 MB/s log file. Furthermore, we will capture the packet data transaction (IP, MAC, source and destination) without capturing raw dataset.

E. Defense IPS Device

There are several project : [7] proposal; development intrusion prevention based SNMP, Integrated with other system defense, and [12] propose the implementation load balancing that developed using libpcap library with clustering technique. Unfortunately, there is no one identify to secure intrusion prevention device from attack.

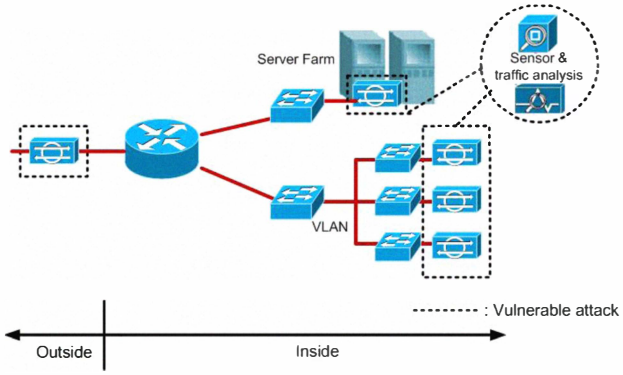

Figure 6, the method distribution Intrusion prevention system. The attacker can do scanning, which in interrogation a topology overall network.

From the attacker sides [16], hackers initiate attacks on target machines through multiple attack actions and mechanisms. These multiple single attack actions belong to an attack plan indeed, which the general steps to attack such as probe, scan, intrusion, and goal.

There are several ways for an attacker to find hole. The step of scanning is tried to find information vulnerable our system, it is can produce information, such as IP Address devices, scheme of topology, application systems of running, etc.

Countermeasure against that is : (i) Connected device uses SSL / HTTPS and access with XML to provide a standardized interface between it, (ii) Block ICMP reply and Enable NAT with limited access IP devices, (iii) uses Transport Layer Security (TLS), (iv) VPN mechanisms, to tunneling between IPS.

F. Sensor Management

The sensor is one of the parts critical to IPS. Unfortunately, capacity and performance of sensor is limited by amount of network traffic, placement of installation, and system uses (hardware or module based). Accordingly, port monitoring with SPAN (Switched Port Analyzer) can be uses to identifying and recognize packet.

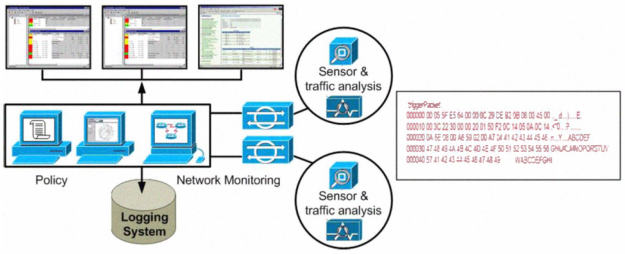

Figure 8, network monitoring collect data management from sensor.

Therefore, monitoring network is easy to change control, alert incident response, create notify administrator, or block traffic immediately. Unfortunately, the main issue is that, there are several standard of proprietary vendor between SNMP version. The past researcher [17], propose integration and encompassing a security infrastructure where multiple security device from a global security layer, which is defined with respect to the others and interact dynamically and automatically with the different security devices.

G. Collaboration

In this section, we discuss to collaboration security system, the Unified *Threat Management* (UTM) respond. UTM can answer the solution. Furthermore, there are several variously technology uses in defense system. Unfortunately, Proprietary vendor is different from each other.

According to CSI/FBI survey [11], the enterprise uses several technology security system, such as (i) anti-virus software 97%, (ii) anti-spyware 80%, (iii) firewall 97%, (iv) IPS 54%, and (v) VPN 85%.

There are three components in the defense system, (i) Web Security, (ii) Network Protection, and (iii) Mail filtering. In the recent years Firewall is one of most technology preventive suspicious threat, such as : VPN, URL Filter, IDS, Email Anti Virus, Signing/encryption, NAC, Encryption, Wireless security, P2P filter, IM filter, and Anti Spyware.

There are several standards default to determine framework requirement security policy, such as ISO 17799, which is to declare, indentify, analyze and describes requirement that must be met to accommodate IPS. The previous researcher declared [17], Information Security Management System (ISMS), it requires regulation standard, which in ISO security standards and government compliance regulations guide and enforce organizations about certain requirements and norm.

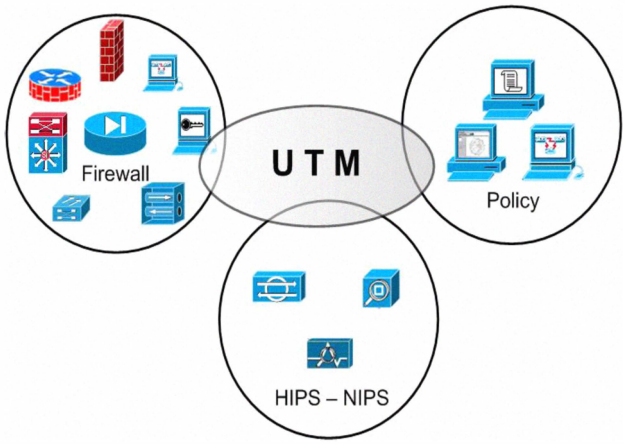

Figure 7. The Unified Threat Management (UTM), which in collaborate heterogeneous defense system (Firewall, IPS) between policy and network monitoring

According to Common Vulnerability Exposure (cve.mitre.org) is a list of intrusion product, there are several IPS devices with proprietary standard. The mechanism need to integrate heterogeneous network. We proposed Unified Threat Management (UTM) to collaborate and integrate between it.

UTM, can do collect all security devices monitoring with one network management. The main collaboration and integration is Firewall, intrusion prevention between policy and network monitoring to one control management.

III. RESULT

In this section, we identify steps anticipated for user and network architecture, as following:

1. Accuracy Signature, in this issue, our suggestion is appropriate selection of signature types, which recognize model that can be use. Embedded in layer 2 and layer 3 devices, which is increase recognized suspicious threat solution.
2. Maximum traffic volume, this is important because any network node can suffer a variety of problems. We suggest observing user and network architecture, such as (i) large enterprise, (ii) branch office, (iii) medium financial enterprise, (iii) medium educational enterprise, or (iv) the small office home office.
3. Topology design, in this issue there are two factors to be affected, *first* is a sensor placement, and *second* is number of sensor, we must identifying as topology needed.
4. Quota usage logging, replication, backup and elimination scheduling is a mechanism to efficiency and effective logging storages. We must Describes how long sensor event logs should be kept, when they should be archived, and where the archive is stored.
5. Protections of IPS device from attack, Countermeasure against unauthorized access from attacker that method distribution IPS.
6. Monitoring of management sensor, installed of sensor directly connected with embedded in the gateway is one of solution, which is the sensor that provides the ability to inspect, identified, recognized and monitoring capability of inbound-outbound of real-time traffic. Furthermore, monitoring sensor uses Network Monitoring Center (NMC) for early prevention status. Which is, the system of use : (i) Ease of Management (ii) Reduces Complexity, and (iii) Simplifies Operation
7. Collaboration of UTM, to collaborate and integrate between heterogeneous defense systems, we proposed UTM mechanism, which in Firewall, IPS between policy and network monitoring to one system management control.

IV. CONCLUSION & FUTURE WORK

IPS, which proactively combines the firewall technique with that of the Intrusion Detection System,. In this paper, we have presented, analyze and identify challenging issue to develop the intrusion prevention, the evaluation of our solution have shown how to avoid anticipation. Future work will focus on accuracy of signature with behavior-based prevention, which is an experiment with our data set of real-traffic network.

REFERENCES

[1] C.M. Akujuobi, et al "Application of Wavelets and Self-similarity to Enterprise Network Intrusion Prevention and Prevention Systems", Consumer Electronics, 2007.

[2] E. Guillen, et al " Weakness and Strength Analysis over Network-Based Intrusion Prevention and Prevention Systems" Communications, 2009.

[3] C. Pattinson, et al,"Trojan Prevention using MIB-based IDS/IPS system", Information, Communication and Automation Technologies, 2009.

[4] E. Carter, et al, "Intrusion Prevention Fundamentals : an introduction to network attack mitigation with IPS", Cisco press, 2006.

[5] Kjetil Haslum, et al," Real-time Intrusion Prevention and Security of Network using HMMs", Local Computer Networks, 2008.

[6] Frias-Martinez.V, et al, "Behavior-Profile Clustering for False Alert Reduction in Anomaly Prevention Sensors " Computer Security Applications Conference, 2008.

[7] Xinyau Zhang, et al, "Intrusion Prevention System Design", Computer and Information Technology, 2004

[8] Martuza Ahmed, et al," NIDS : A Network based approach to intrusion prevention and prevention", International Association of Computer Science and Information Technology - Spring Conference, 2009.

[9] Yaping Jiang, et al ,"A Model of Intrusion Prevention Base on Immune", Fifth International Conference on Information Assurance and Security, 2009.

[10] Rainer Bye, et al, "Design and Modeling of Collaboration Architecture for Security", International Symposium Collaborative Technologies and Systems, 2009.

[11] Robert Richardson, "CSI Computer Crime & Security Survey 2008", 2008.

[12] Anh Le, et al," On Optimizing Load Balancing of Intrusion Prevention and Prevention Systems", IEEE, INFOCOM Workshops, 2008

[13] Kamei, S, et al," Practicable network design for handling growth in the volume of peer-to-peer traffic", Communications, Computers and signal Processing, 2003.

[14] D. Stiawan, A.H. Abdullah, M.Y. Idris, "The Measurement Internet Services", International Conferences, ICGC-RCICT, 2010.

[15] Taras Dutkevych, et al, " Real-Time Intrusion Prevention and Anomaly Analyze System for Corporate Networks, IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, 2007.

[16] Zhijie Liu, et al, " Correlating Multi-Step Attack and Constructing Attack Scenarios Based on Attack Pattern Modeling", International Conference on Information Security and Assurance, 2008.

[17] Sourour.M, et al, "Collaboration between Security Devices toward improving Network Defense", sevent IEEE/ACIS International Conference on Computer and Information Science, 2008.