State University of Campinas
School of Electrical and Computer Engineering

IntelFlow: A Proactive Approach To Add Cyber Threat Intelligence To Software Defined Networks

September 22, 2015

Student: Javier Richard Quinto A.
Orientator: Prof. Dr. Christian Esteve Rothenberg

Outline

1. Motivation & Background
2. Problem Definition & Research Objectives
3. Proposed Architecture: IntelFlow
4. Proof of Concept Implementation
5. Final Results
6. Conclusions

Motivation

Source: [1]

Motivation

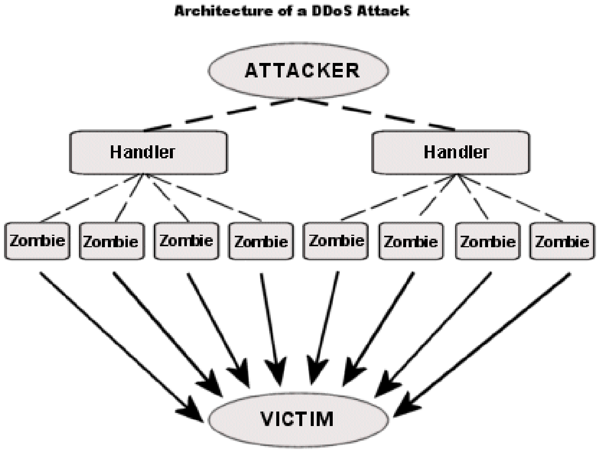
Source: [1]

Source: [2]

Motivation

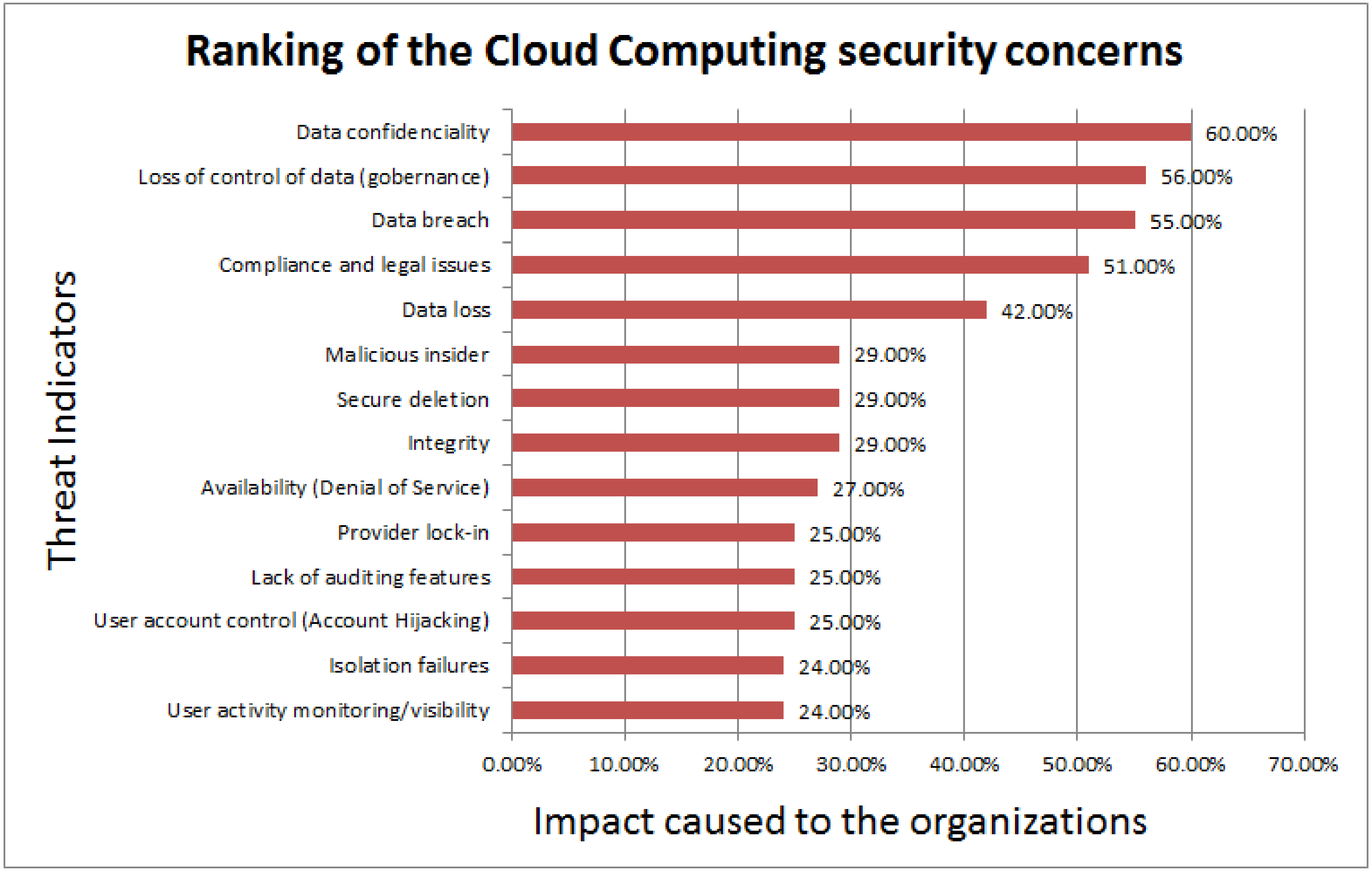
Source: [1]

Source: [2]



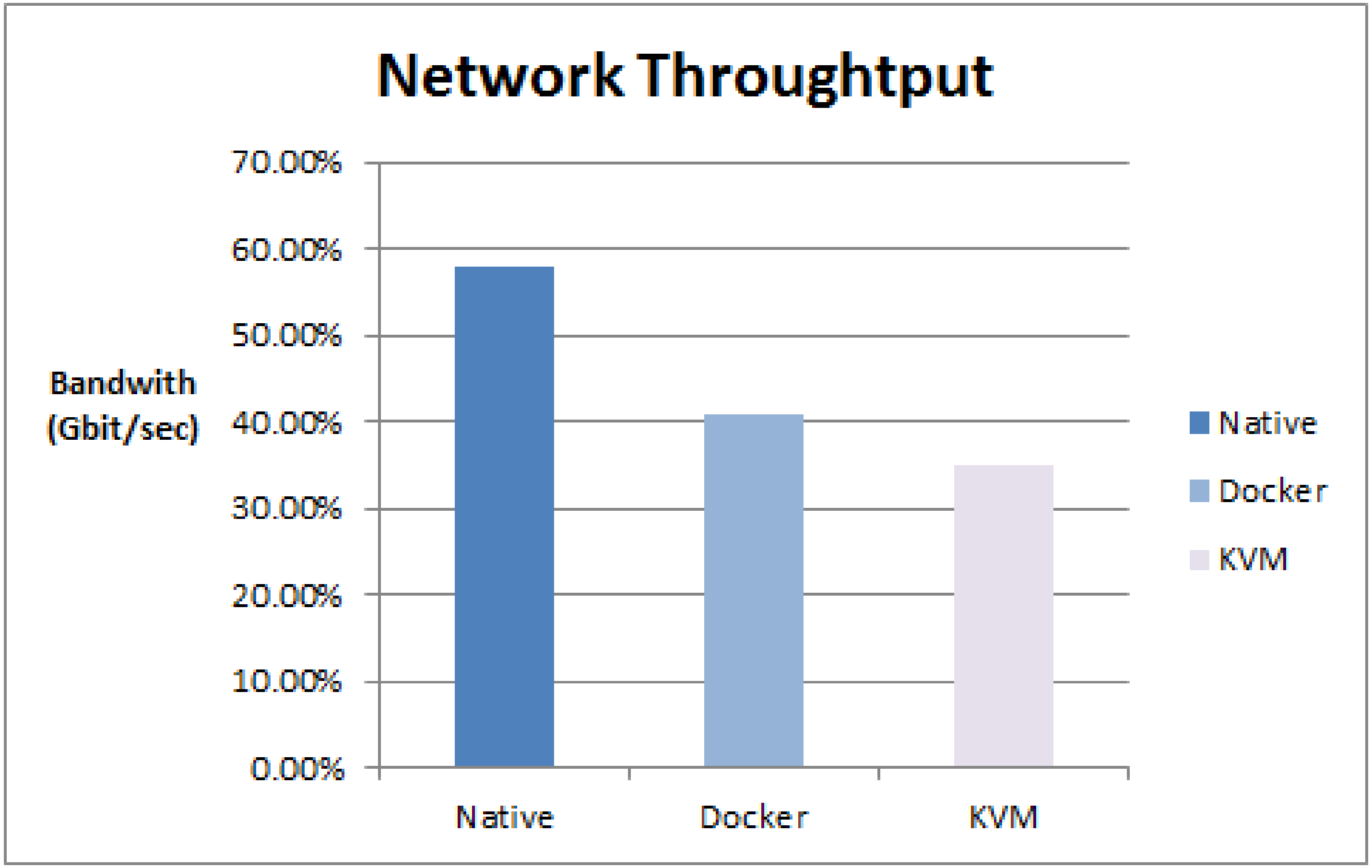
Source: [3]

Motivation



Cloud computing top threats. Adapted from data avaliable in [1]

Motivation



Network Throughtput
Bandwith (Gbit/sec)
70.00%
60.00%
50.00%
40.00%
30.00%
20.00%
10.00%
0.00%
Native
Docker
KVM
Native
Docker
KVM

Background

What is Intruder Detection System ?

IDS is a security device that monitor network or computer in order to analyze and detect malicious attacks within a networking system.

Detection Techniques of the IDSs

Anomaly: Identifies events which do not agree to an expected pattern or is an unusual event. However, new rules are difficult to create.

Signature: Monitors packets on the network and compare them against a database of signatures or attributes. However, new attacks can not be detected.

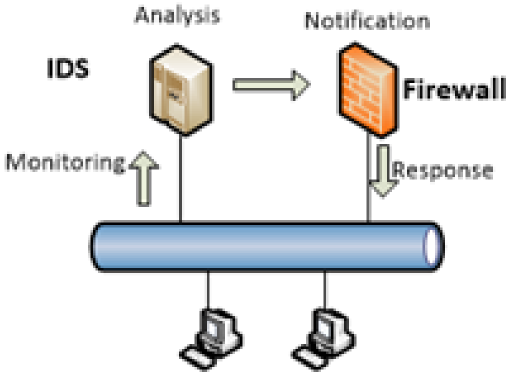


Fig: Components IDS

Background

What is Intruder Detection System ?

IDS is a security device that monitor network or computer in order to analyze and detect malicious attacks within a networking system.

Detection Techniques of the IDSs

Anomaly: Identifies events which do not agree to an expected pattern or is an unusual event. However, new rules are difficult to create.

Signature: Monitors packets on the network and compare them against a database of signatures or attributes. However, new attacks can not be detected.

Bro is a type of IDS powerful network analysis framework that is much different from the typical IDS. Bro is adaptable, efficient, flexible, forensics, in-depth analysis, highly stateful, open source.

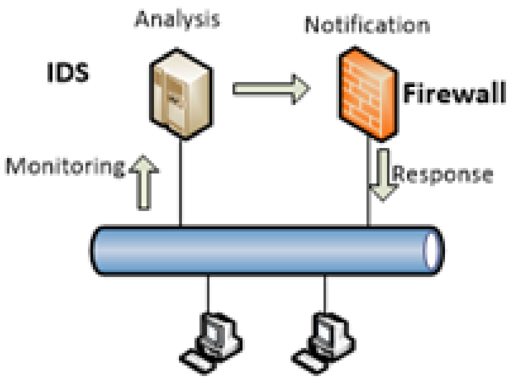


Fig: Components IDS

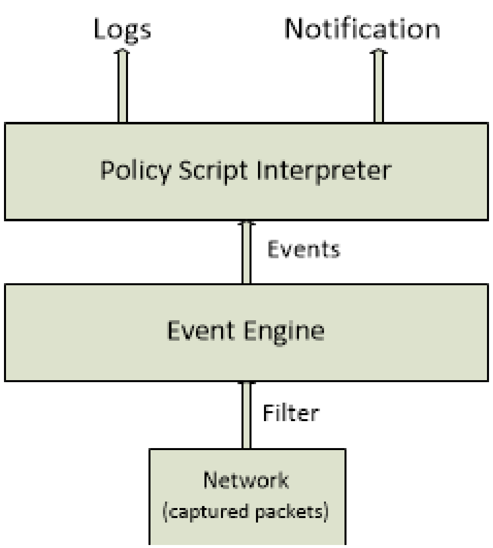


Fig: Architecture BRO IDS

Source: [3]

Motivation

Limitation of the Intruder Prevention System (IPS)

IPS is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits. However, it has certain limitations such as:

a)**Latency**: Deep Packet Inspection degrades the performance and results in a high latency.
b)**Accuracy**: Reducing false positives is a challenge.
c)**Flexibility**: Blocking certain range of the suspect network without affecting the healthy traffic from innocent neighbors.

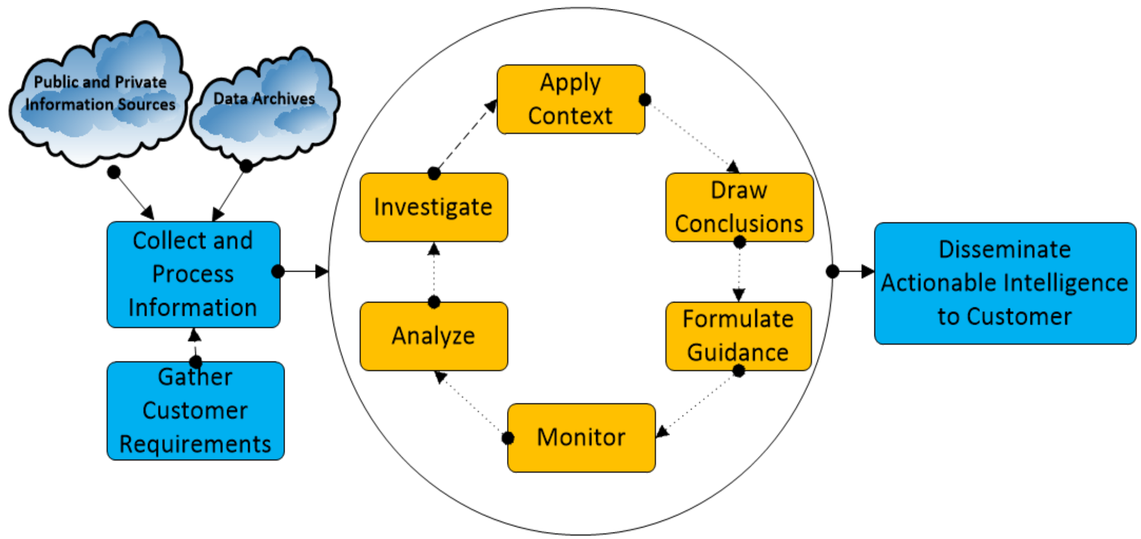
Motivation

Information vs Intelligence

Raw Information
Source: [4]

Motivation

Information vs Intelligence



Raw Information
Source: [3]

Intelligence Data
Source: [4]

Background

What is Cyber Threat Intelligence ?

Cyber Threat Intelligence (CTI) is an emerging methodology of evidence-based knowledge, that organizations identifies and successfully responds to a cyber attack. E.g., When an institution faces a similar threat, they are able to rapidly deploy countermeasures based on the experience acquired by other organizations, in order to prevent attacks intelligently.

Fig: Cyber Threat Intelligence
Source: [5]

Background

What is Cyber Threat Intelligence ?

Cyber Threat Intelligence (CTI) is an emerging methodology of evidence-based knowledge, that organizations identifies and successfully responds to a cyber attack. E.g., When an institution faces a similar threat, they are able to rapidly deploy countermeasures based on the experience acquired by other organizations, in order to prevent attacks intelligently.

Fig: Cyber Threat Intelligence
Source: [5]

Collective Intelligence Framework (CIF) is a cyber threat intelligence management system that allows you to combine known malicious threat information from many sources and use that information for identification (incident response), detection (IDS) and mitigation (null route).

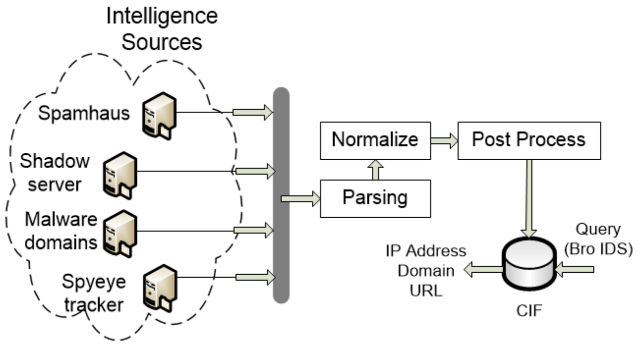


Fig: Process of the CIF

Problem Definition & Research Objectives

Problem Definition

- **General:** How to enhance network defense technologies?
- **More specific:** How to integrate Cyber Threat Intelligence into (software-defined) networking management and control systems?

Problem Definition & Research Objectives

Problem Definition

•**General:** How to enhance network defense technologies?
•**More specific:** How to integrate Cyber Threat Intelligence into (software-defined) networking management and control systems?

Scope and Objectives:

a)Leverage Collective Intelligence Framework (CIF) to add security service to SDN.
b)Integrate the Bro's Intel framework to acquire intelligence data from reliable sources.
c)Evaluate the IntelFlow architecture for different scenarios, validating it with a proof-of-concept implementation and experiments to assess effectiveness and performance.

Background

What is Software Defined Networking (SDN) ?

- The control and data planes are decoupled.
- Forwarding decisions are flow-based, instead of destination-based.
- Control logic is moved to an external entity, the SDN controller located on Network Operating System (NOS).
- The network is programmable through software applications running on top of the NOS that interacts with the underlying data plane devices.

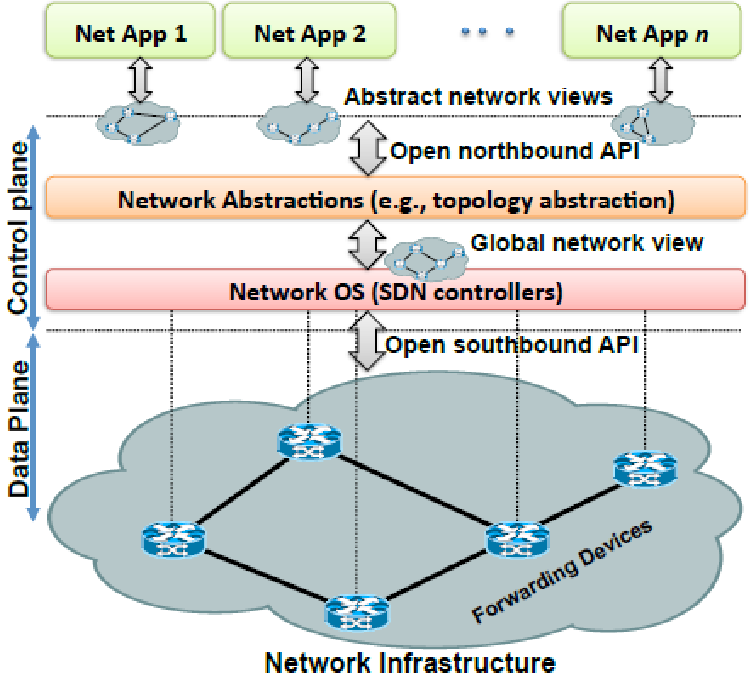


Fig: SDN architecture
Source: [6]

Background

What is OpenFlow?

OpenFlow is the first standard communications interface defined between the control and forwarding layers of an SDN architecture.

The protocol allows direct access to and manipulation of the forwarding plane of network devices such as switches and routers.

This allows moving network control out of the networking switches to logically centralized control software.

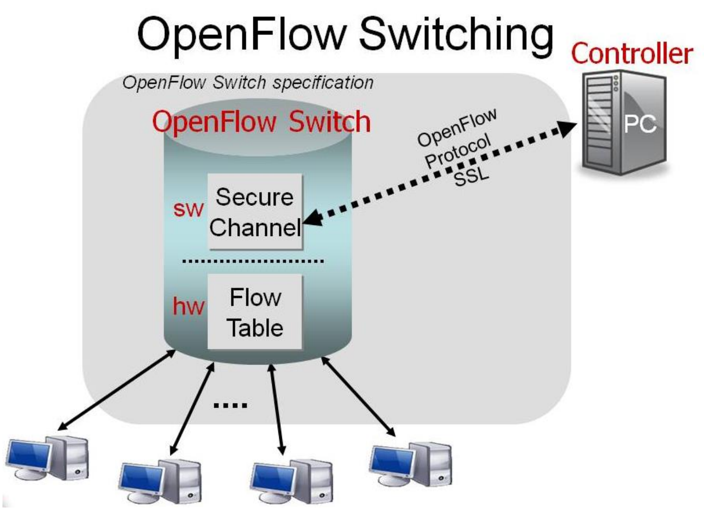


Fig: SDN / OpenFlow

Source: [7]

Related Work

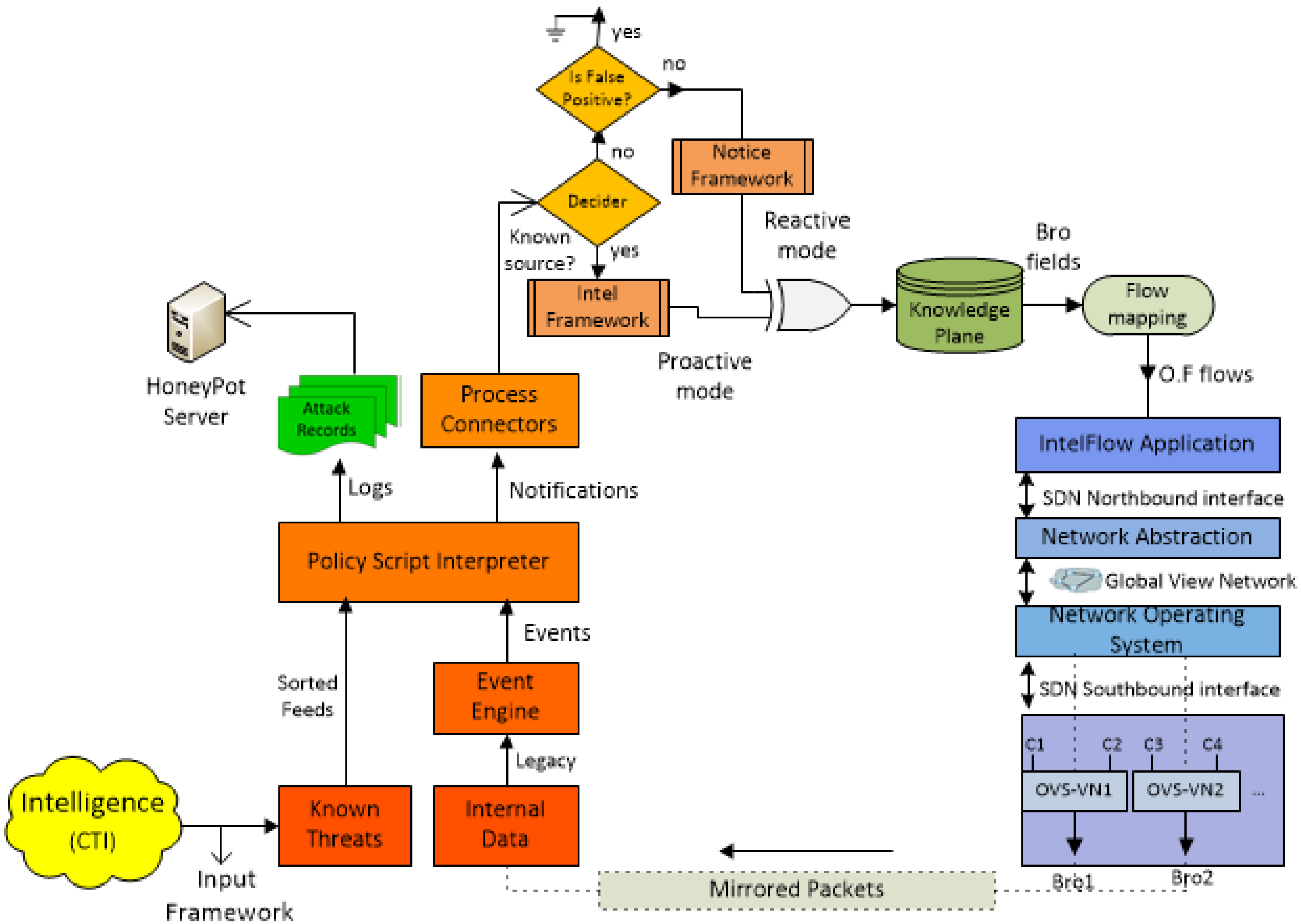
Name	Operation Mode	Inter domain	Controller	Countermeasure
SnortFlow [17]	Reactive	No	POX	Performance evaluation about SnortFlow agent deployed at Dom 0 is better than at Dom U for about 40 %
BroFlow [14]	Reactive	No	POX	Effective detecting DoS attacks caused by flooding and blocking attacks from its origin. Reducing delay at to 10 times on the networks under the attack and ensures the delivery of useful packets in the maximum rate of the link.
Elastic [16]	Reactive	No	POX	Blocking a malicious flow; evaluation of resources consumed for packet analysis and elasticity overload and discharge in Detecting Module intrusion.
IPSFlow [19]	Proactive	No	Undefined	Automatic blocks malicious traffic close to the orign
DefenseFlow [20]	Proactive	No	ODL, Cisco, etc	DDoS protection as a native network service and collect statistics
SciPass [23]	Reactive and Proactive	No	Owner	Improve transfer performance and reducing load on network infrastructure. Load balancing, bypass rules to avoid forwarding good data through firewalls of good data
IntelFlow	Reactive and Proactive	Yes	any	Detect and prevent certain threats on networks by a proactive mode and deploying countermeasures to the threats learned through the CTI which lead to the networking infrastructure layer being reconfigured through flow table updates to the data plane switches

Proposed Architecture: IntelFlow

Main idea: Introducing a Knowledge Plane (KP)

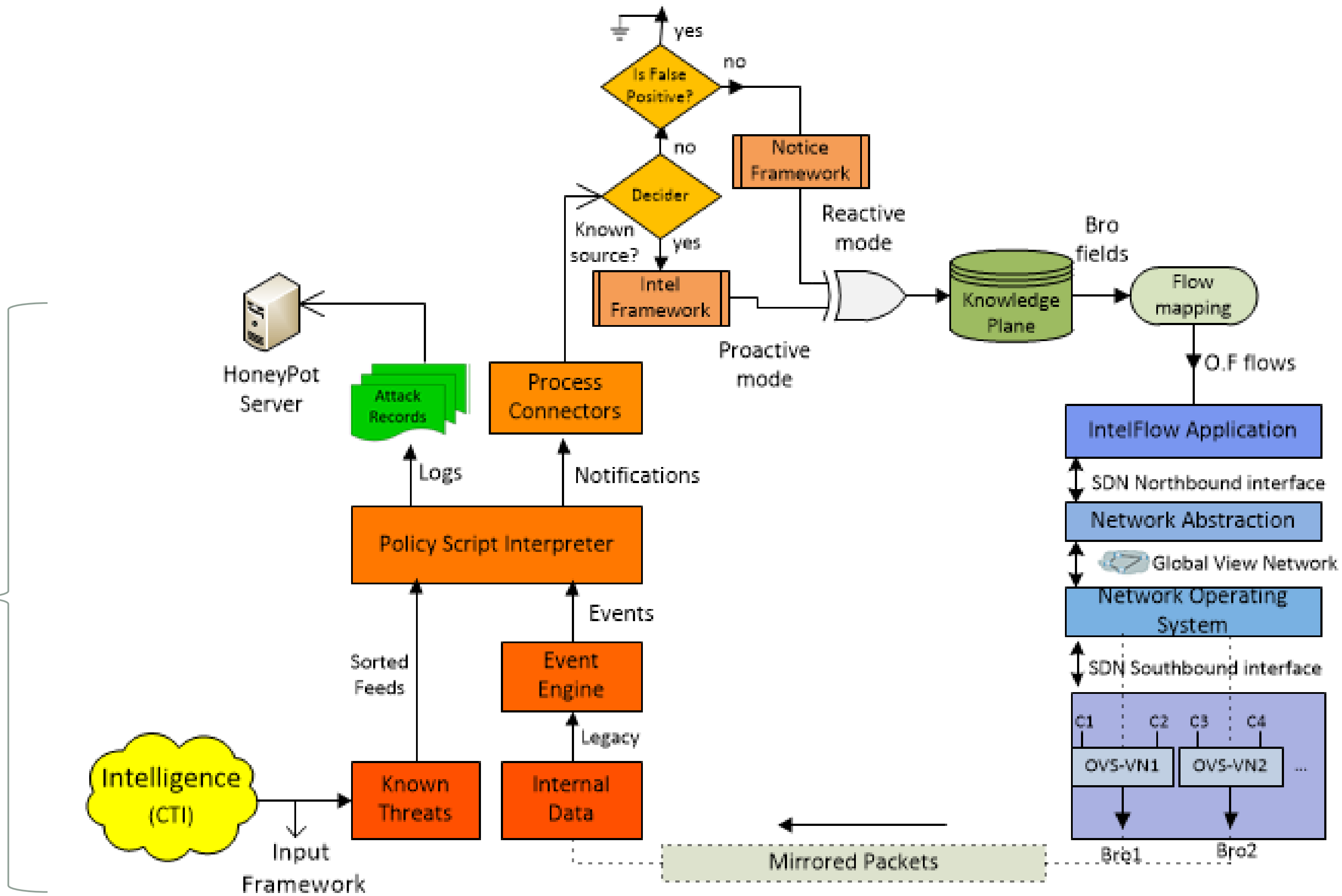
- KP receives as input sources of threat intelligence
- KP allows queries from Bro IDS about the acquired intelligence data.
- KP exports the generated OpenFlow rules.

Proposed Architecture: IntelFlow

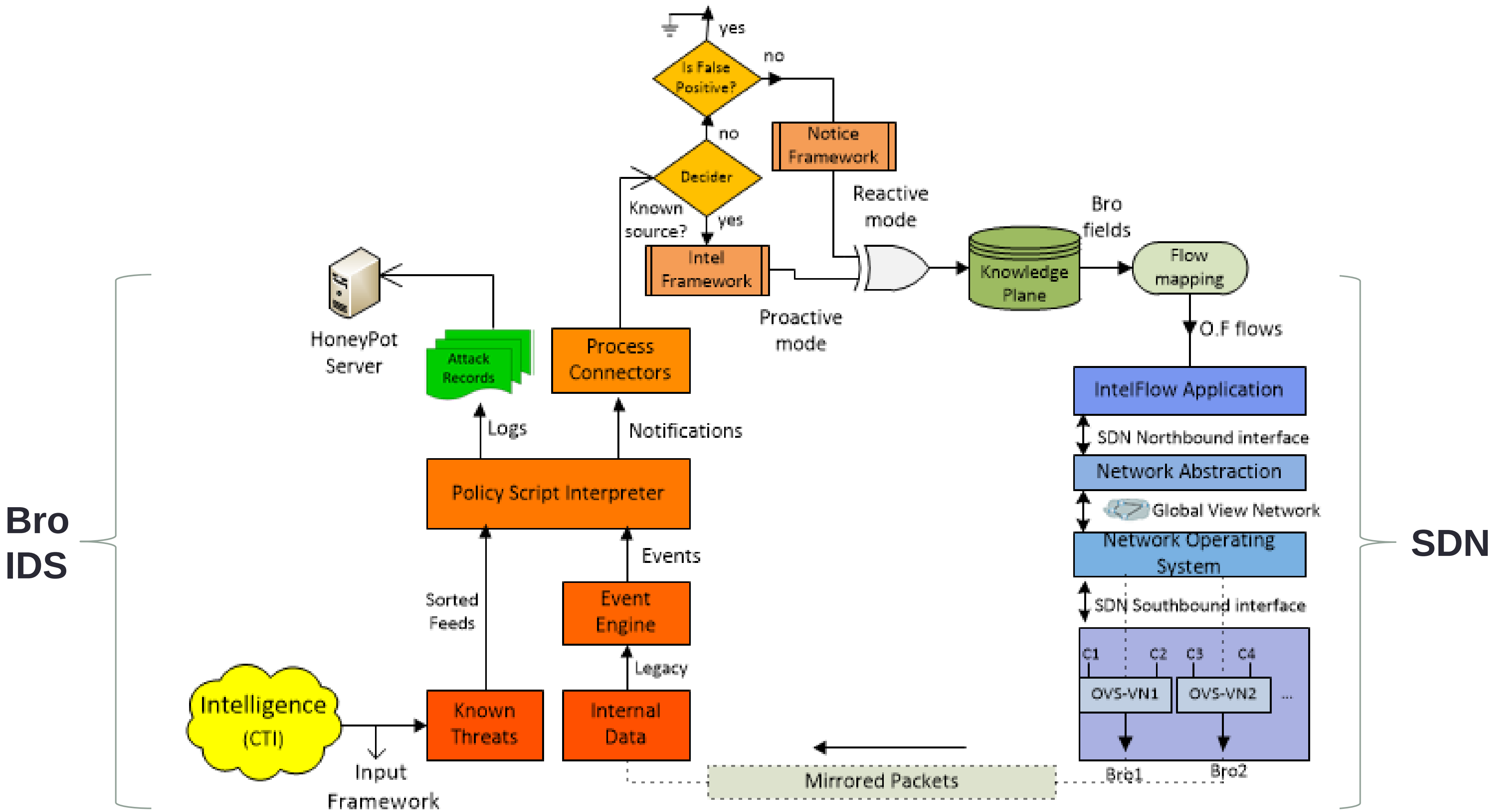


Proposed Architecture: IntelFlow

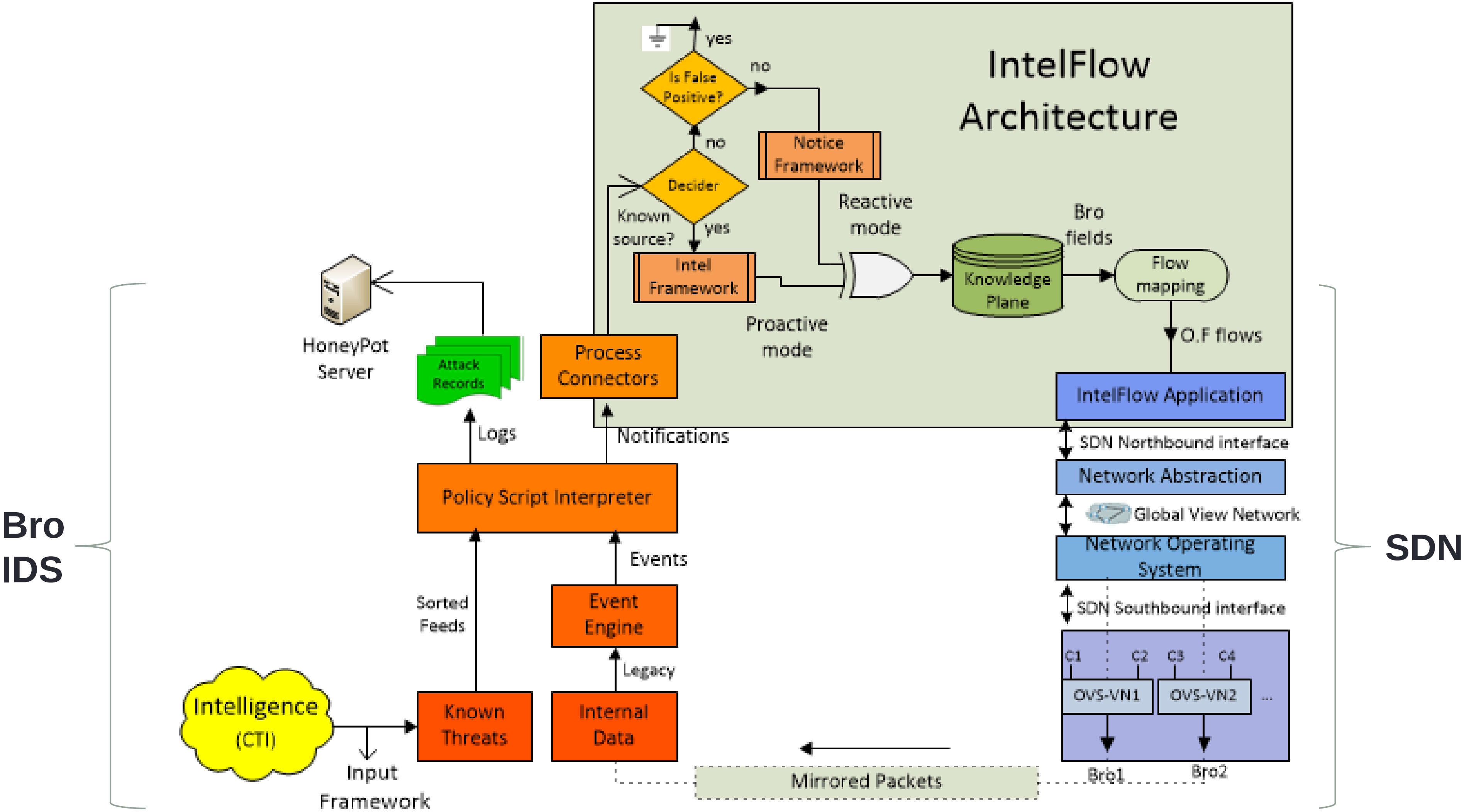
Bro IDS



Proposed Architecture: IntelFlow



Proposed Architecture: IntelFlow



Mode of Operation

Reactive	Proactive
• Controller as **requester** and the application as a **responder**. • **Receive** notifications from controller when an event occur.. • Interface ***listener*** which are able to receive notifications from the controller when certain events occur. • When a switch receives unknown packets, these are encapsulated in **PacketIN** and send to the controller.	• Controller as **responder** and the application as a **requester**. • **Retrieve** the network information such as domains, sws, and hosts • Interface **flow pusher**, which allows the application to set flows on switches when a certain stimulus is executed. • When a stimulus from external events (Bro IDS) notify to the application to set actions on the controller (**output, normal, drop**).

Intelligence Sources

- **Malware Domain List (MLD)**
- **Malware Domains**
- **Alienvault**
- **Spamhaus**
- **Zeustracker**

Intelligence Types (Indicators of Compromise)

- **IP address**
- **Domain**
- **URL**
- **Software**
- **Email Address**
- **User_Name**
- **File_Hash**
- **File_Name**
- **Cert_Hash**

Intelligence Types (Indicators of Compromise)

- **IP address**
- **Domain**
- **URL**

Indicator types used by **IntelFlow**

- **Software**
- **Email Address**
- **User_Name**
- **File_Hash**
- **File_Name**
- **Cert_Hash**

Architecture (Input Fields)

Bro IDS Input Fields

Field	Description
id.orig_h	Source IP
id.orig_p	Source port
id.resp_h	Destination IP
id.resp_p	Destination port
seen.indicator	Trigger the match
seen.indicator_type	Indicator type (ADDR, DOMAIN)
seen.where	Location where the event was triggered.

Indicator Types

Indicator Type	Localization
Intel::ADDR	Conn::IN_ORIG, Conn::IN_RESP
Intel::DOMAIN	HTTP::IN_HOST_HEADER
Intel::URL	HTTP::IN_URL

Architecture (Input Fields)

Bro IDS Input Fields

Field	Description
id.orig_h	Source IP
id.orig_p	Source port
id.resp_h	Destination IP
id.resp_p	Destination port
seen.indicator	Trigger the match
seen.indicator_type	Indicator type (ADDR, DOMAIN)
seen.where	Location where the event was triggered.

Indicator Types

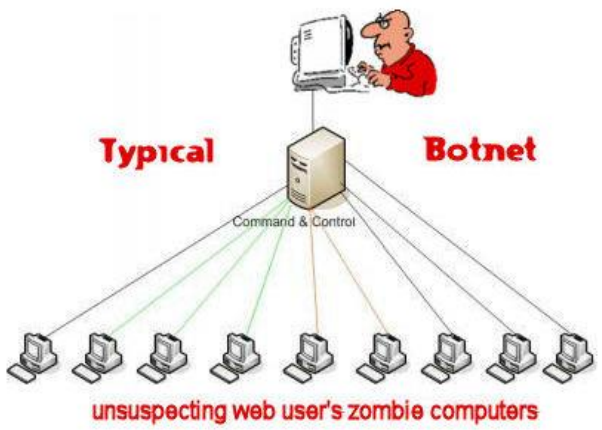
Indicator Type	Localization
Intel::ADDR	Conn::IN_ORIG, Conn::IN_RESP
Intel::DOMAIN	HTTP::IN_HOST_HEADER
Intel::URL	HTTP::IN_URL

Architecture (Outputs Flows)

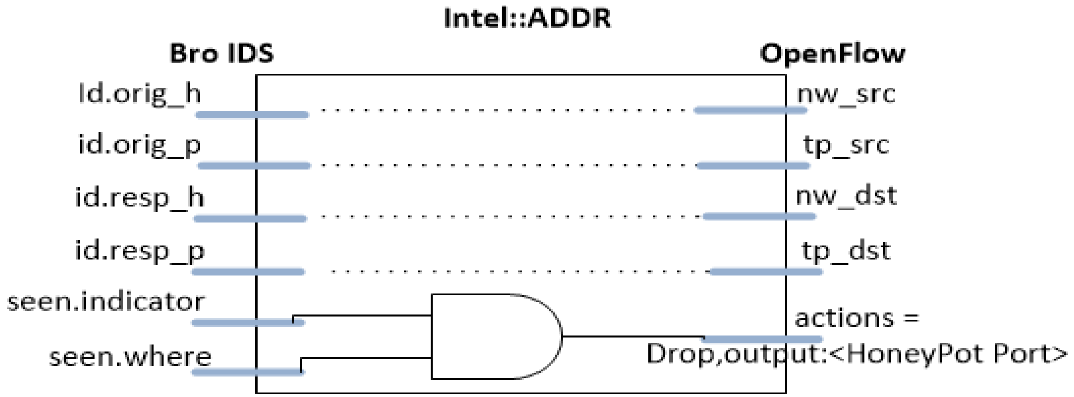
Bro IDS Input Fields

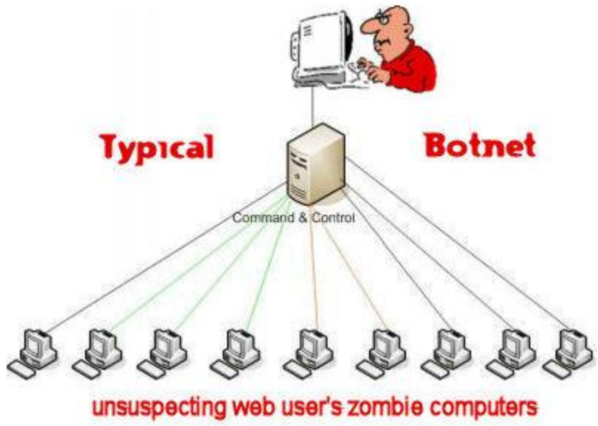
	Field	Value used	Description
	nw_src	any	Match the source IP
	nw_dst	any	Match the TCP source port
Match field	tp_src	any	Match the destination IP
	tp_dst	any	Match the TCP destination port
	dl_type	0x800	Match ethernet protocol type
	nw_proto	6	Match IP protocol type
	nodeid	any	Bridge's mac address
Priority	priority	0-65535	The order that one entry will match in comparison to another
	actions	any	List of actions done on a packet when its entry has been matched

Algorithm for Indicator Type = “Intel::ADDR”



Algorithm for Indicator Type = “Intel::ADDR”

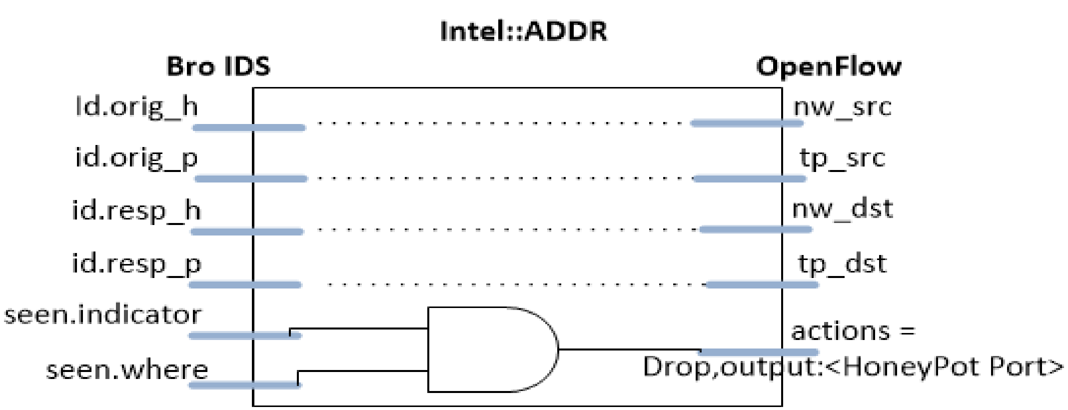


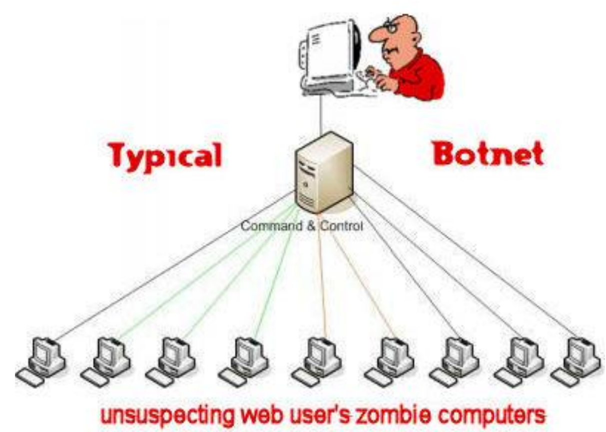


Algorithm for Indicator Type = "Intel::ADDR"

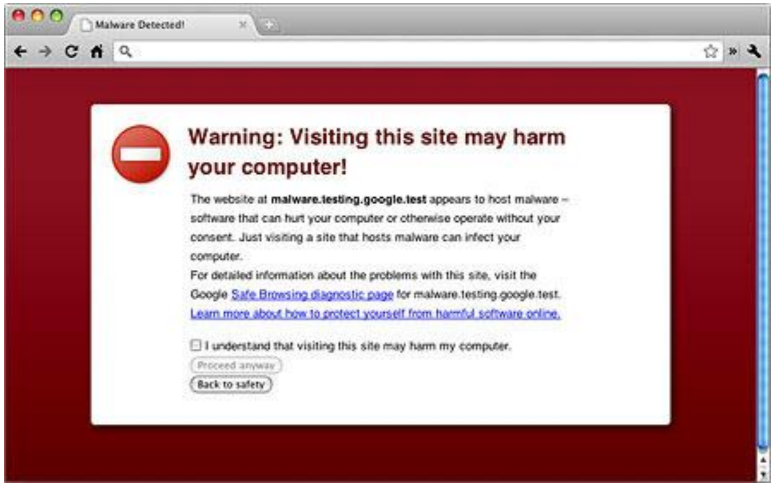
If (seen.where == **Conn::IN_RESP**)
    seen.indicator = **id.resp_h**
    if (seen.indicator) ∈ **KP**
        Nothing to do
    else if
    { actions: Drop(nw_dst) and forward it to a HoneyPot, then Includes the indicator to **KP** }
else if (seen.where == **Conn::IN_ORIG**)
    seen.indicator = **id.orig_h**
 if (seen.indicator) ∈ **KP**
        Nothing to do
    else if
    { actions: Drop(nw_src) and forward it to a HoneyPot, then Includes the indicator to **KP** }

Intelligence Algorithm

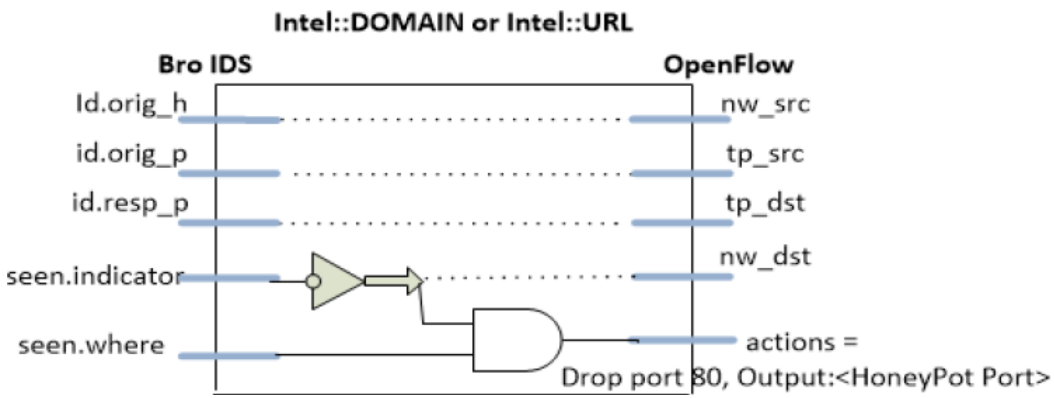


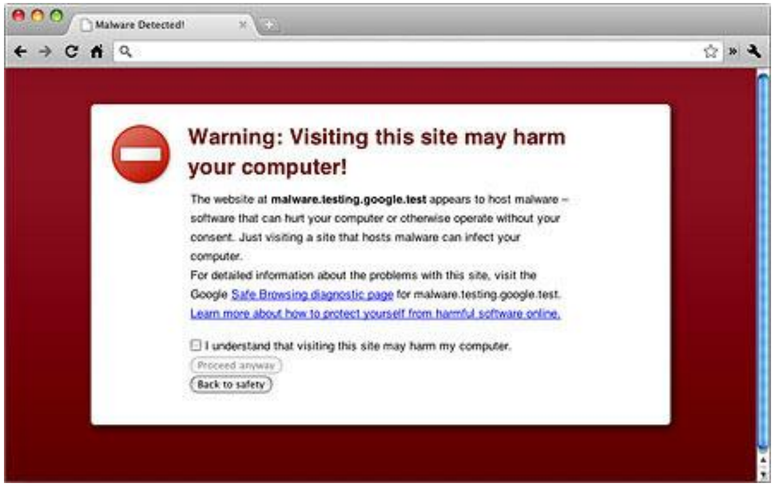


Algorithm for Indicator Type = “Intel::DOMAIN,URL”



Algorithm for Indicator Type = "Intel::DOMAIN,URL"

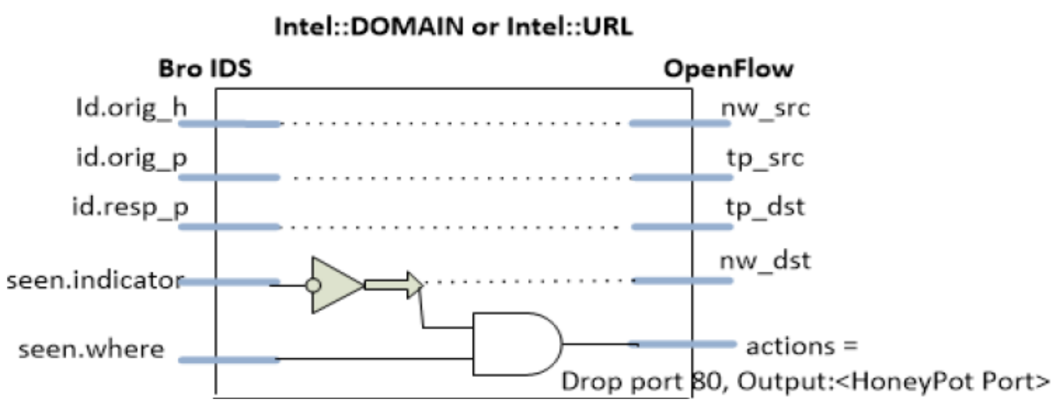


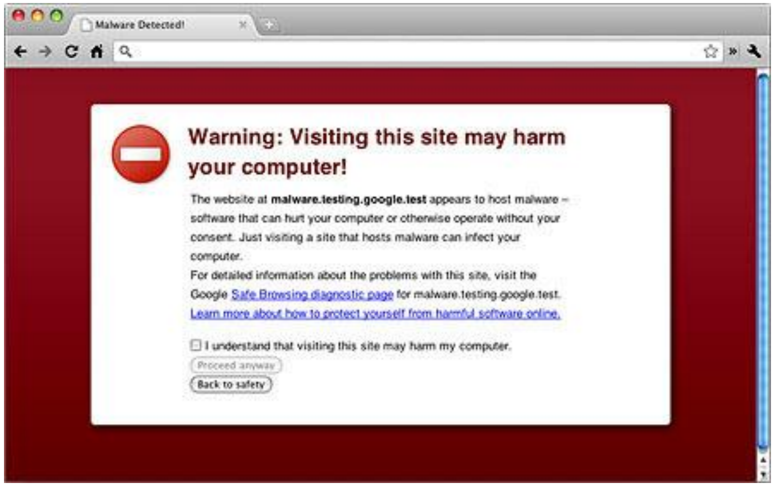


Algorithm for Indicator Type = "Intel::DOMAIN,URL"

If (seen.where == **HTTP::IN_HOST_HEADER** || **HTTP::IN_URL**)
seen.indicator = **malicious_domain**
inverse (seen.indicator) = **malicious_IP**
if (seen.indicator) ∈ **KP**
Nothing to do
else if
{ actions: Drop(**malicious_IP**) and forward it to HoneyPot
then Including the indicator to **KP** }

Intelligence Algorithm

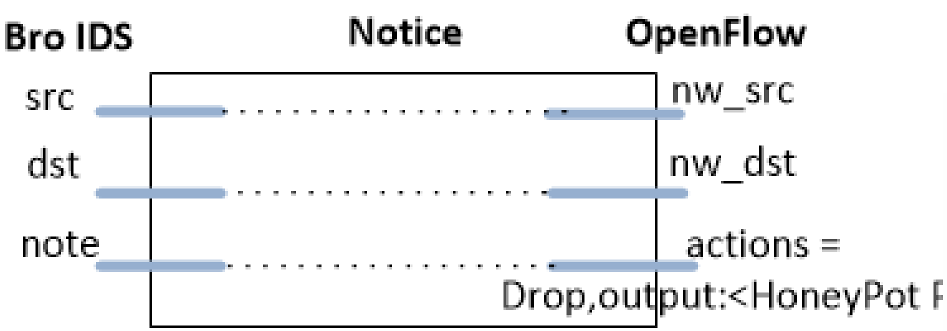




Algorithm for Indicator Type = "Notice"

Algorithm for Indicator Type = "Notice"

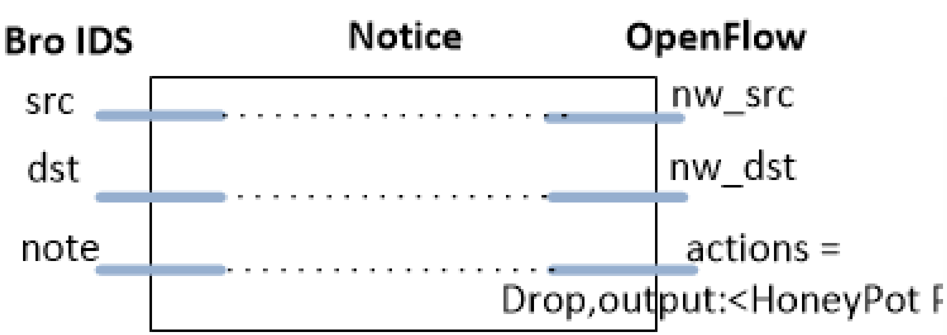
Algorithm for Indicator Type = "Notice"



Algorithm for Indicator Type = “Notice”

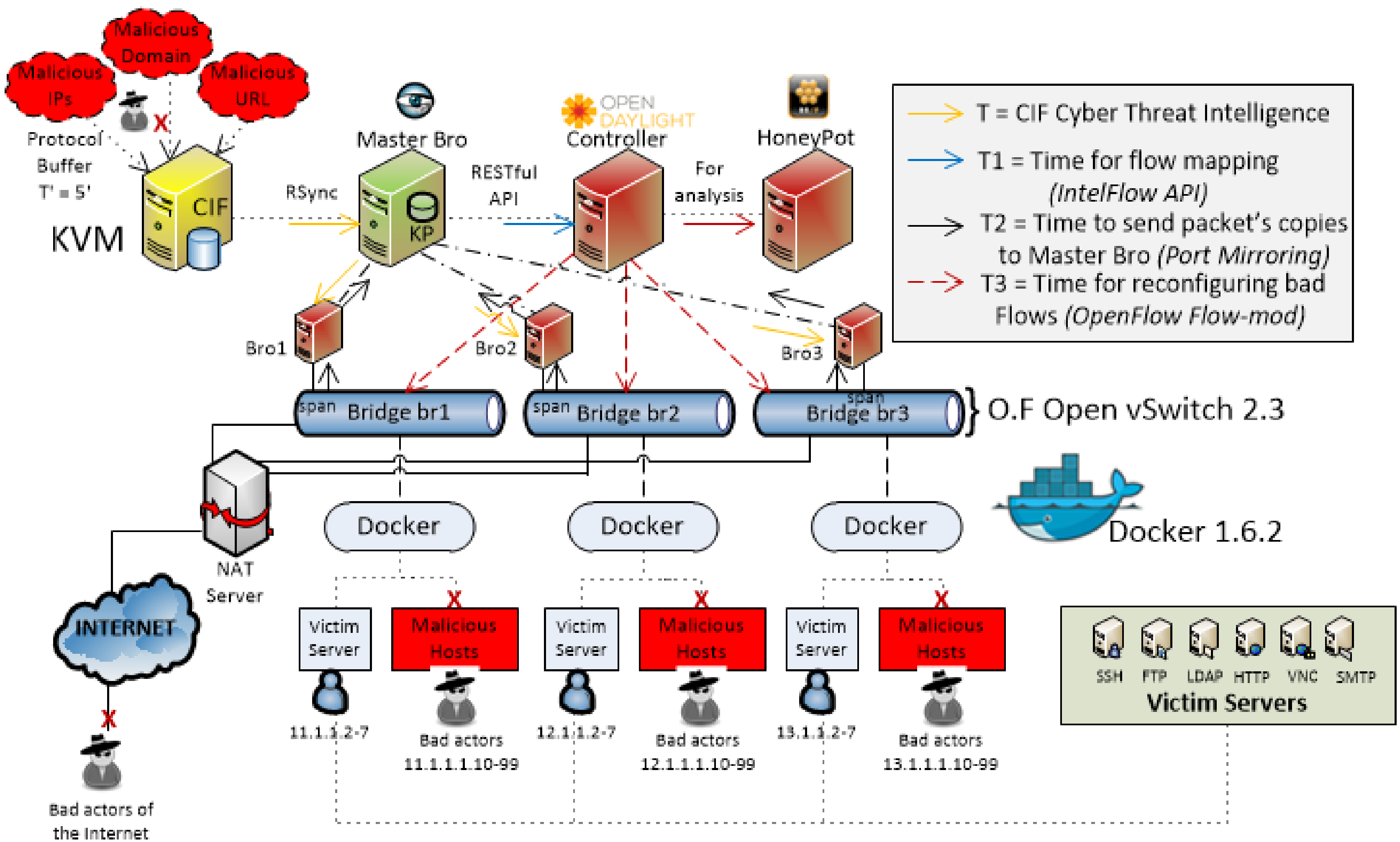
If (note == **Scan::Port_Scan**)
src = **suspicious_IP**
function (src)
if -> false_positive
return 0; // end
else if
mapping (src) = nw_src
actions: Drop(**nw_src**) and forward it to HoneyPot
else If (note == **Scan::Password_Guessing**)
src = **malicious_IP**
mapping (src) = nw_src
actions: Drop(**nw_src**) and forward it to HoneyPop

Notice Algorithm



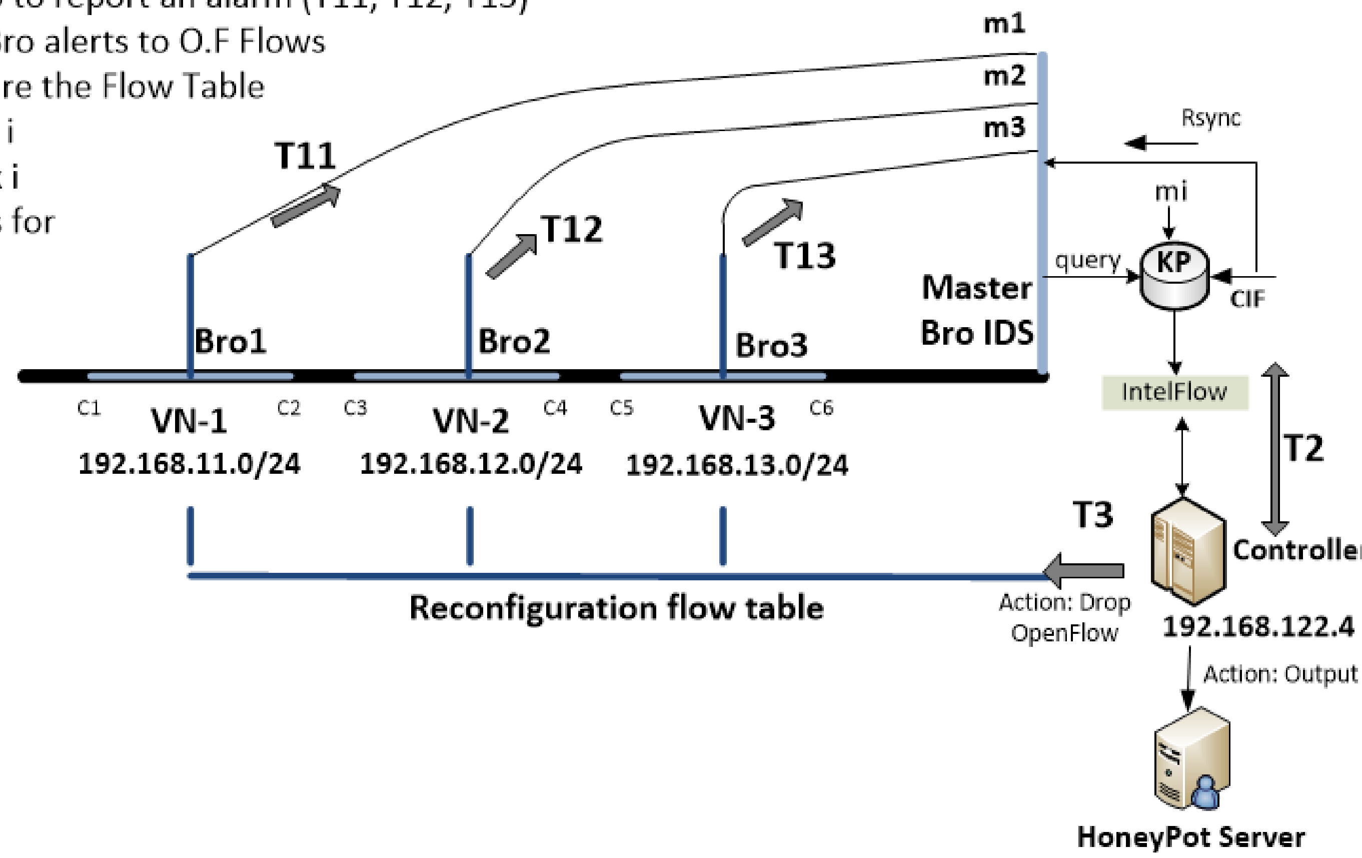
Proof of Concept Implementation

(Test bed)

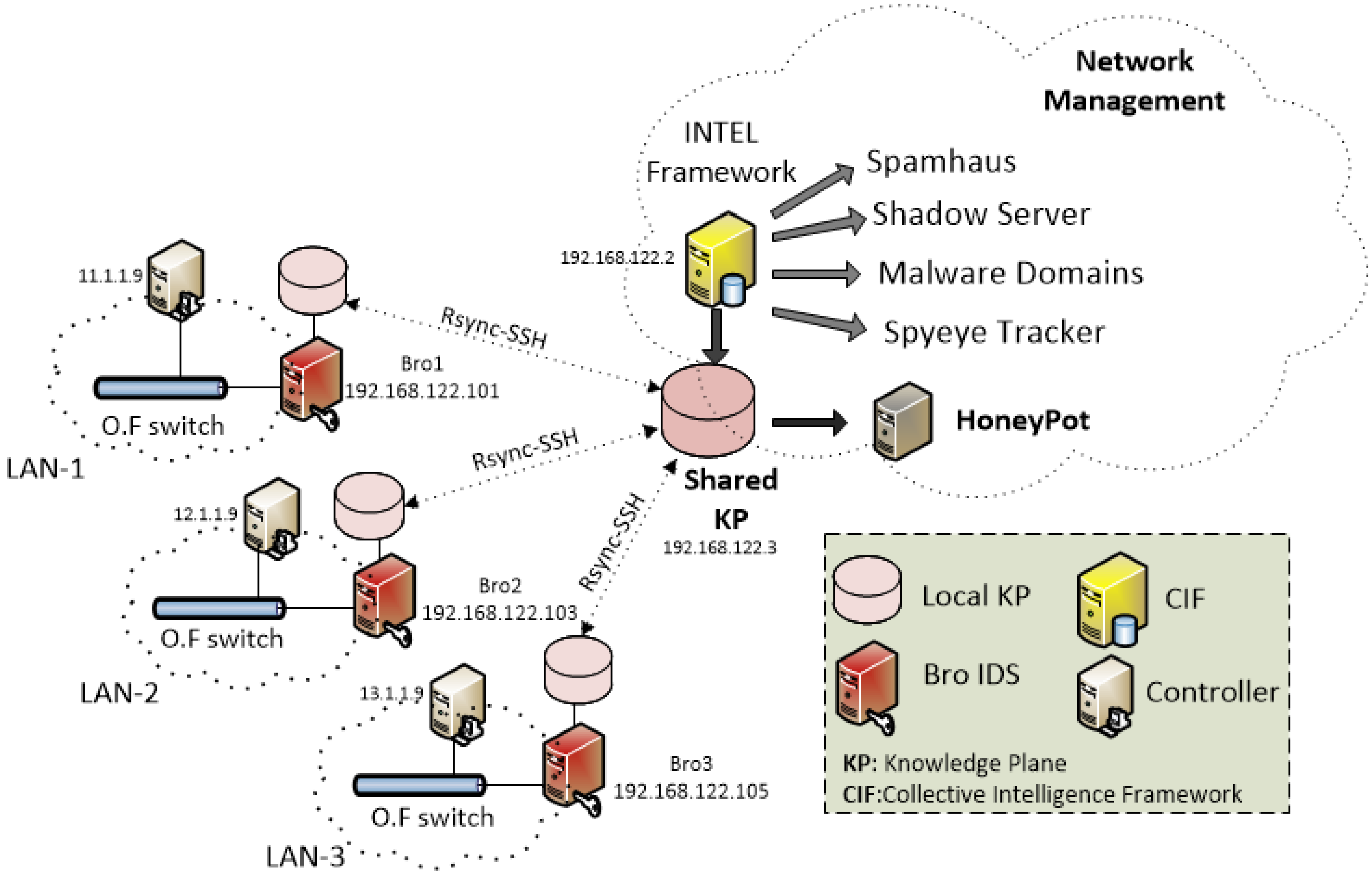


Intra-domain Scenario

T1i: Time used by Bro to report an alarm (T11, T12, T13)
T2: Time to convert Bro alerts to O.F Flows
T3: Time to reconfigure the Flow Table
Ci: Docker Container i
VN-i: Virtual Network i
mi: Alert of messages for
VN-1, VN-2, VN-3



Inter-domain Scenario

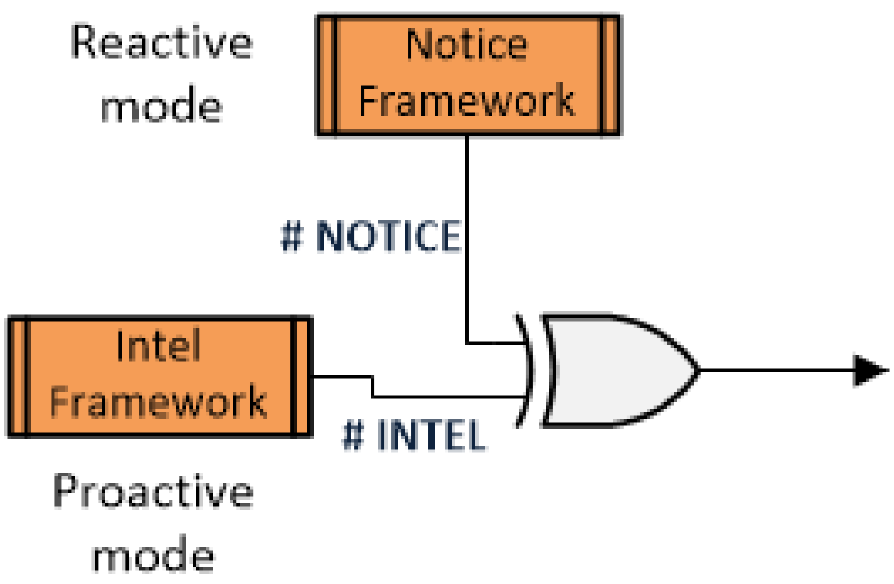


Experimental Methodology

Metrics	Description
# O.F Flows	OpenFlow flow numbers
# INTEL	Known threat detected by Intel Framework
# NOTICE	Malicious event detected by Notice Framework

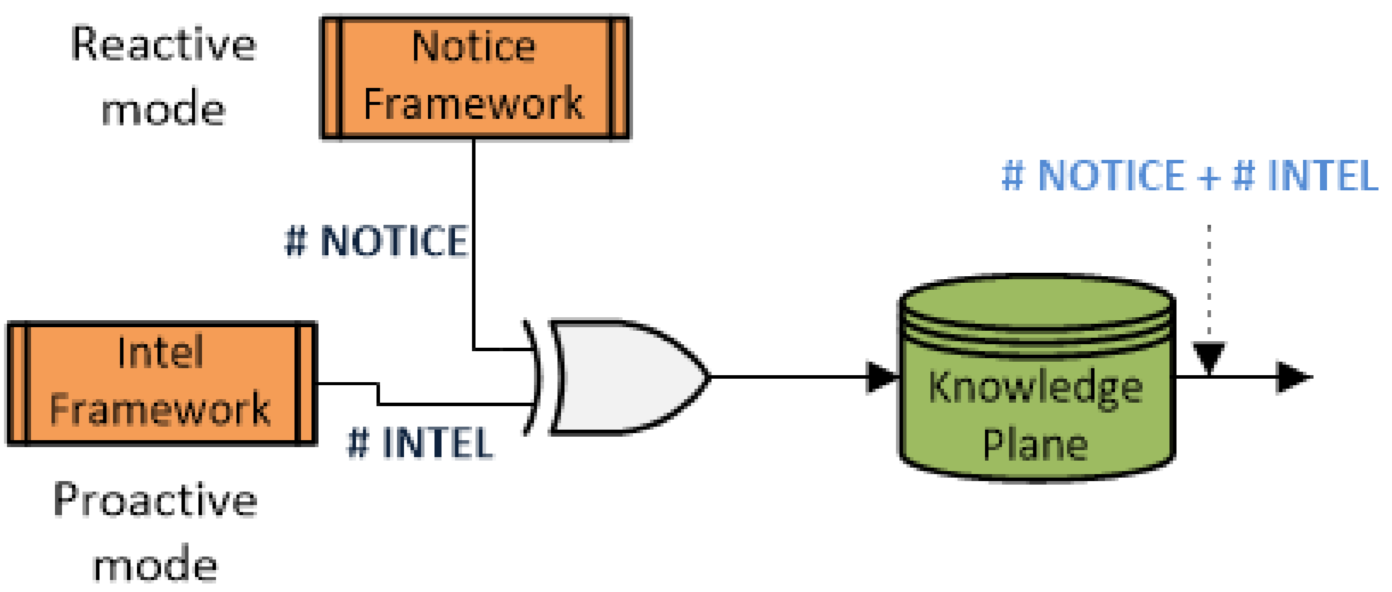
Experimental Methodology

Metrics	Description
# O.F Flows	OpenFlow flow numbers
# INTEL	Known threat detected by Intel Framework
# NOTICE	Malicious event detected by Notice Framework



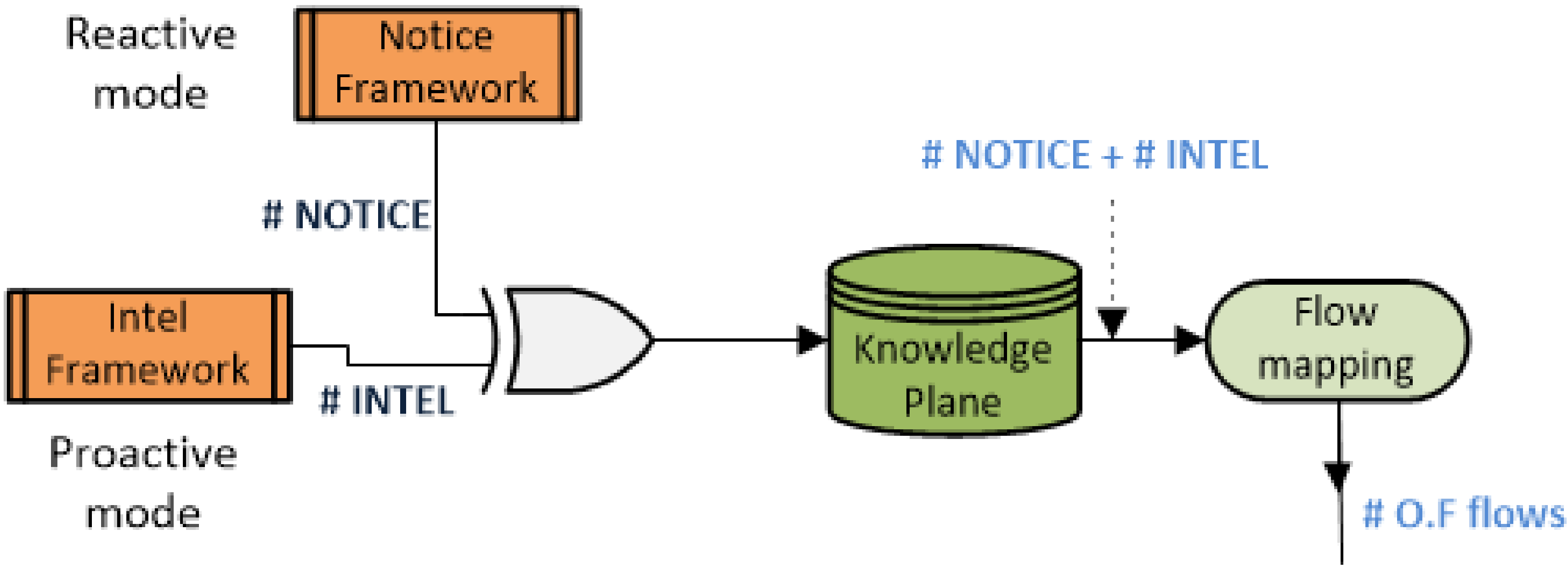
Experimental Methodology

Metrics	Description
# O.F Flows	OpenFlow flow numbers
# INTEL	Known threat detected by Intel Framework
# NOTICE	Malicious event detected by Notice Framework



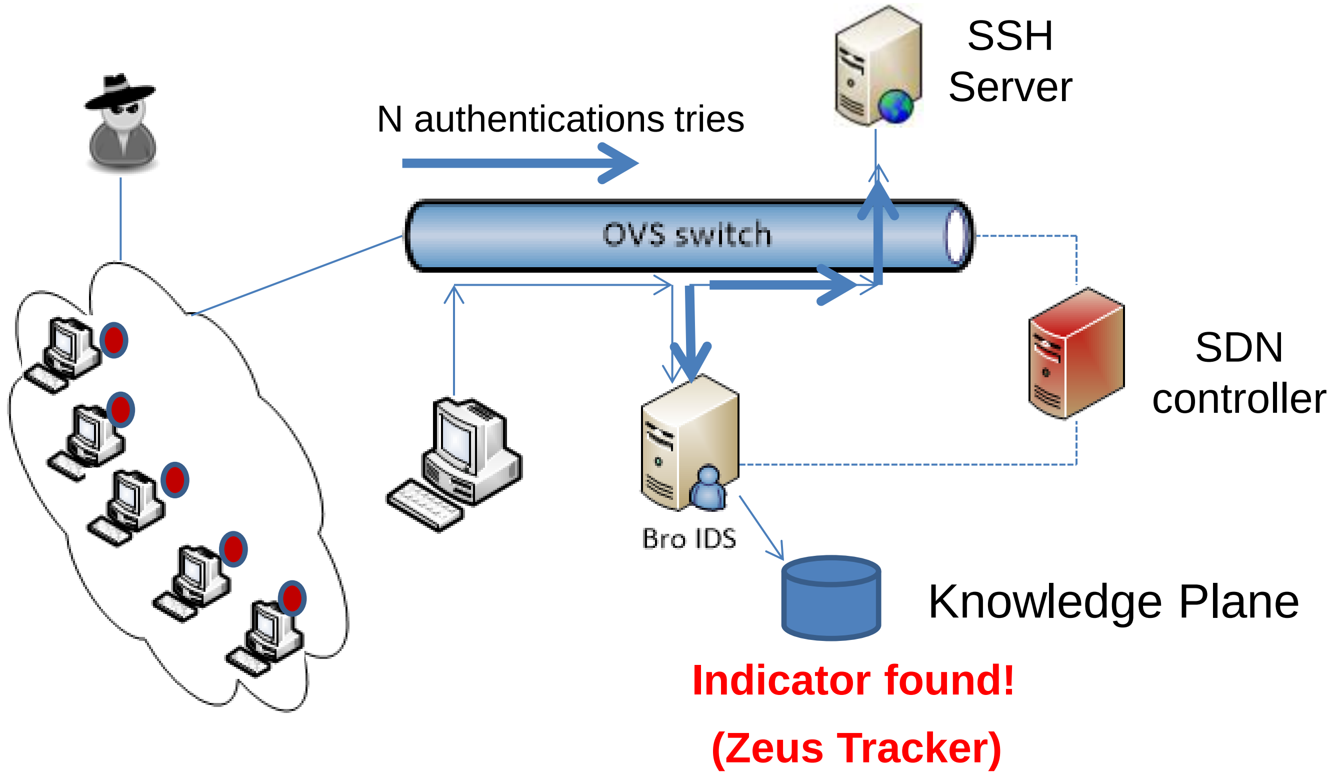
Experimental Methodology

Metrics	Description
# O.F Flows	OpenFlow flow numbers
# INTEL	Known threat detected by Intel Framework
# NOTICE	Malicious event detected by Notice Framework



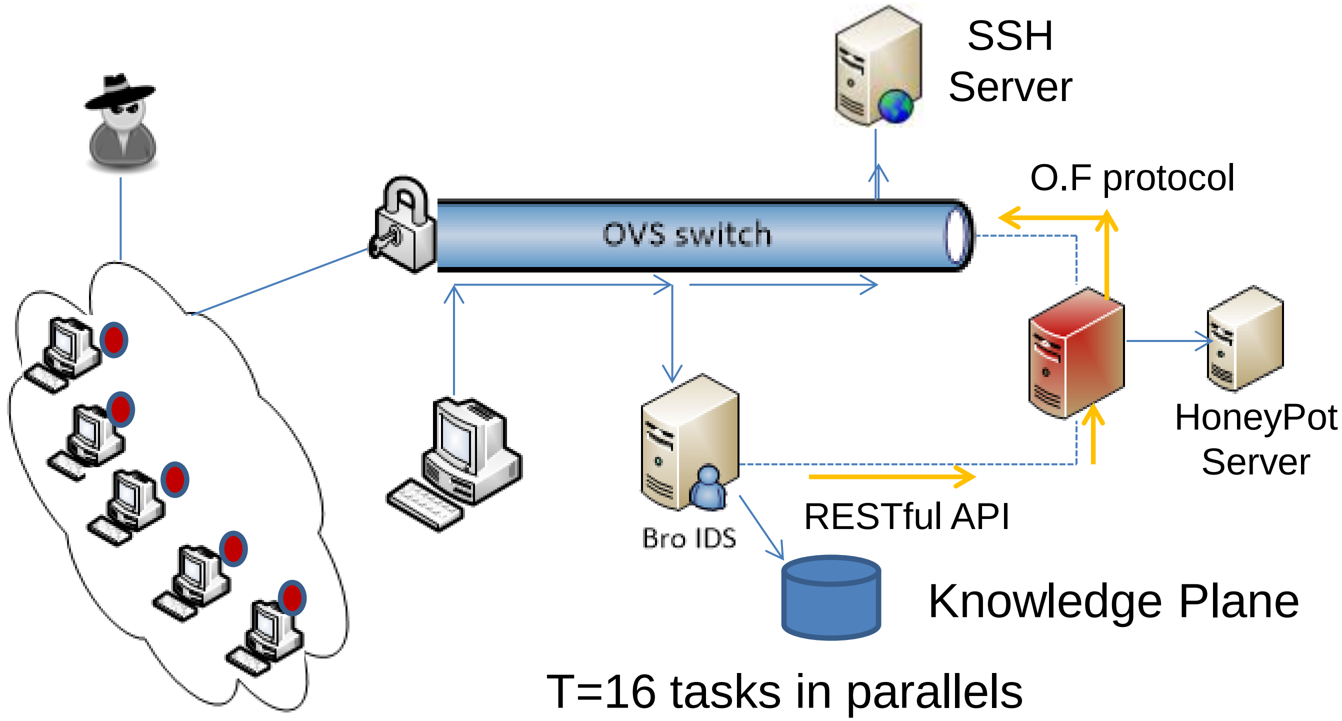
Experimental Evaluation 1

Methodology to counter password guessing-based attacks

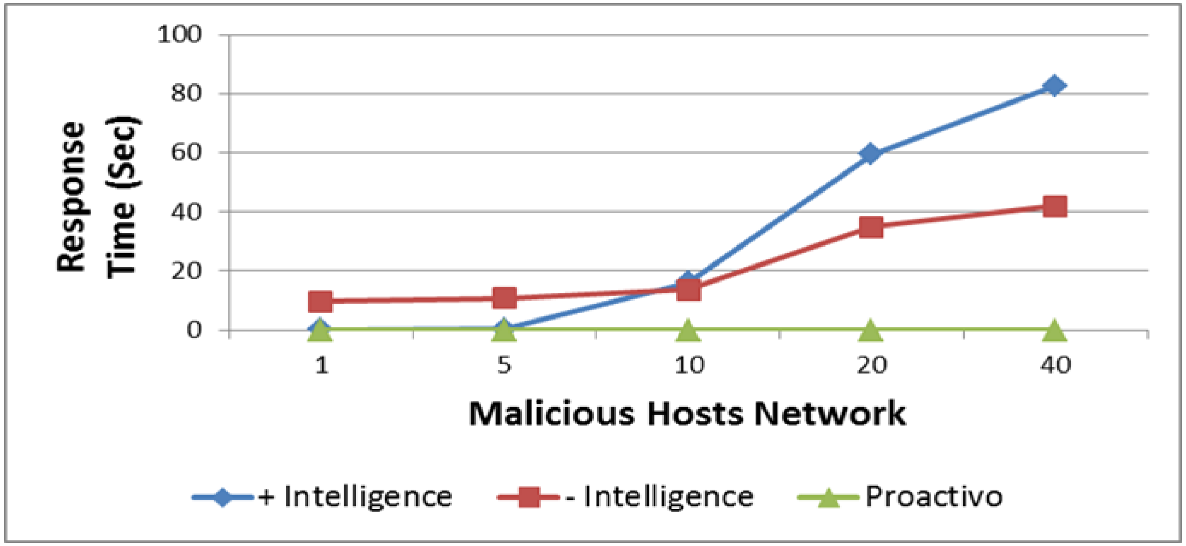


Experimental Evaluation 1

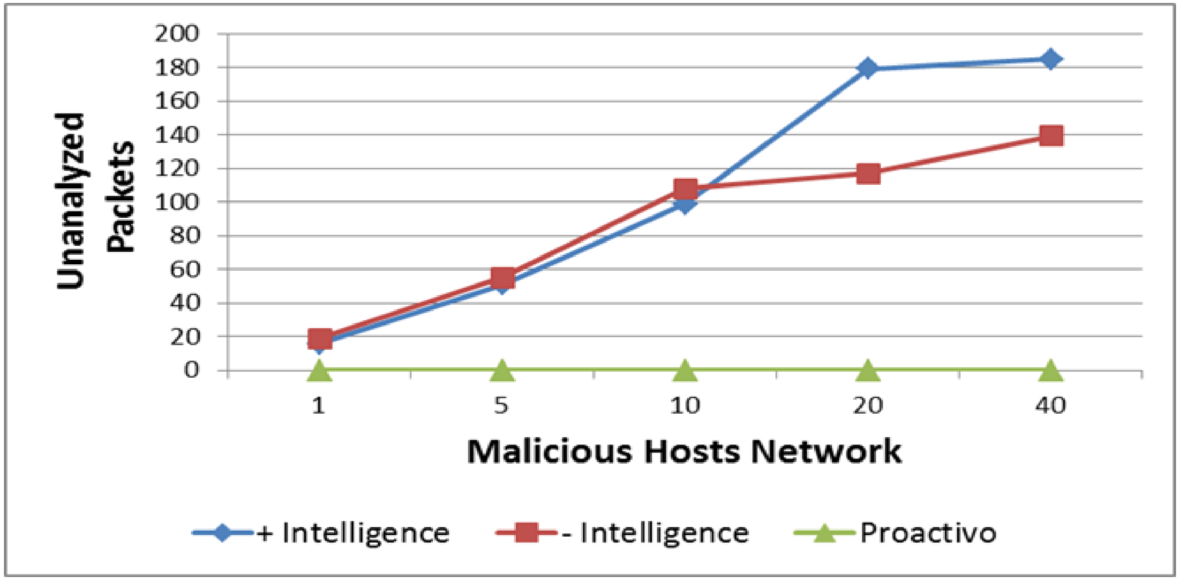
Methodology to counter password guessing-based attacks



T=16 tasks in parallels
5 malicious hosts launching brute-force attacks
With Intelligence: 0.48 seconds
Without Intelligence: 10.77 seconds



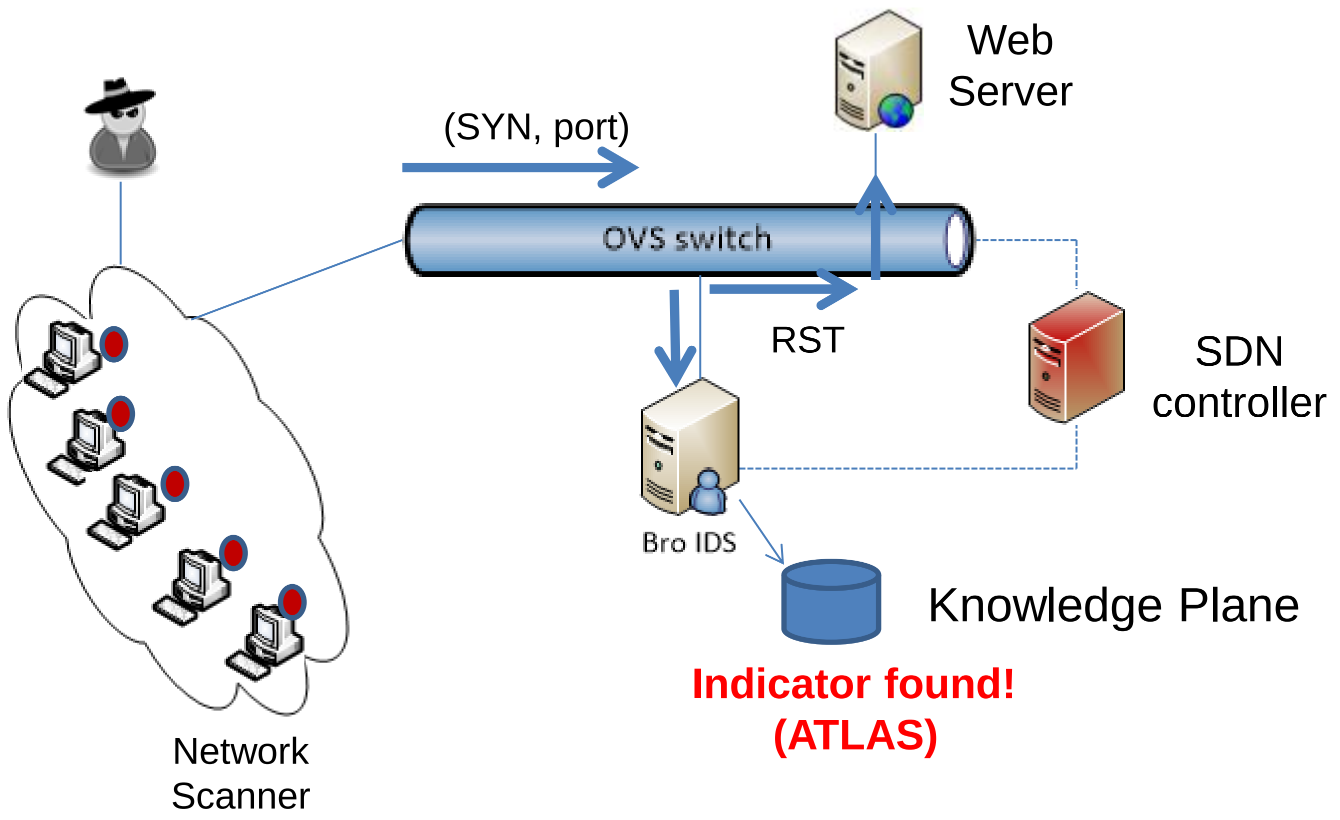
Comparison of the response time varying the amount of malicious hosts



Comparison of the unanalyzed packets varying the amount of malicious hosts

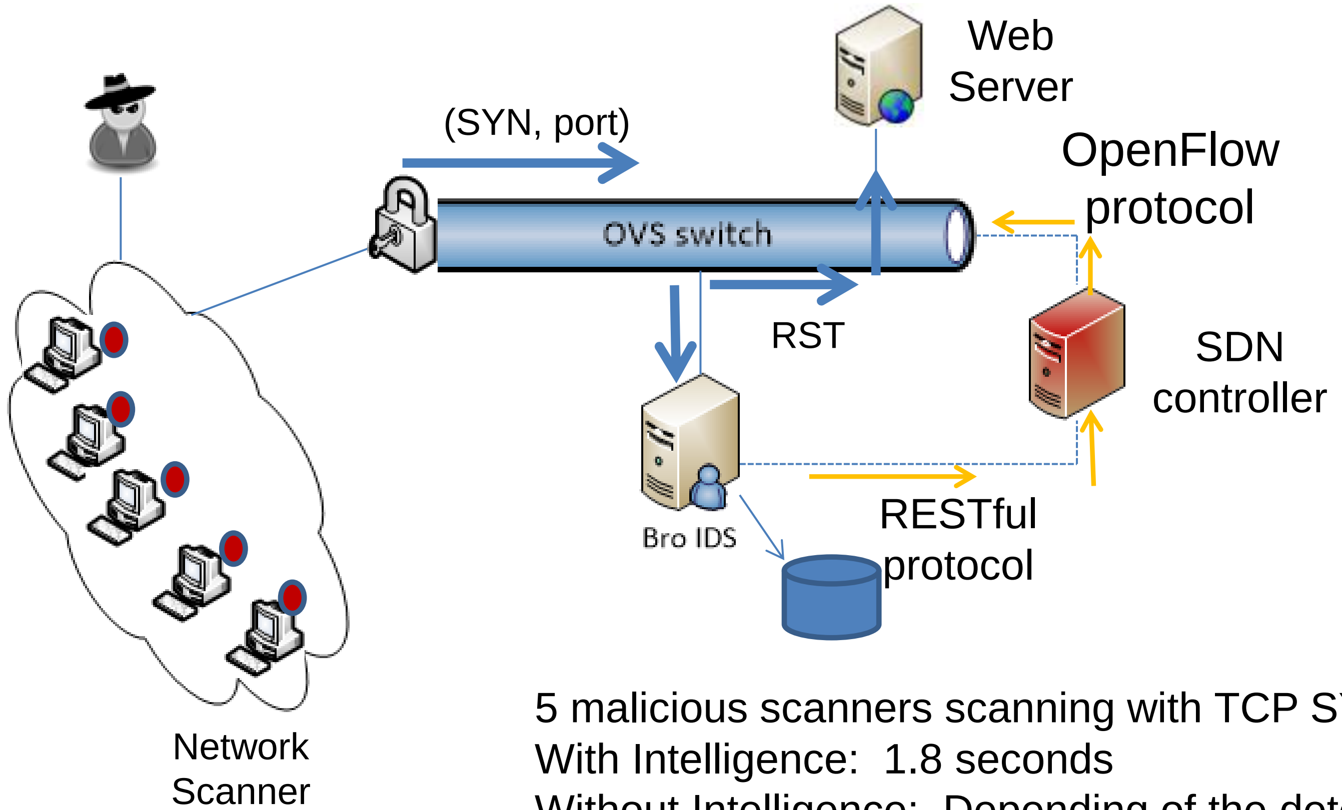
Experimental Evaluation 2

Methodology to counter password guessing-based attacks



Experimental Evaluation 2

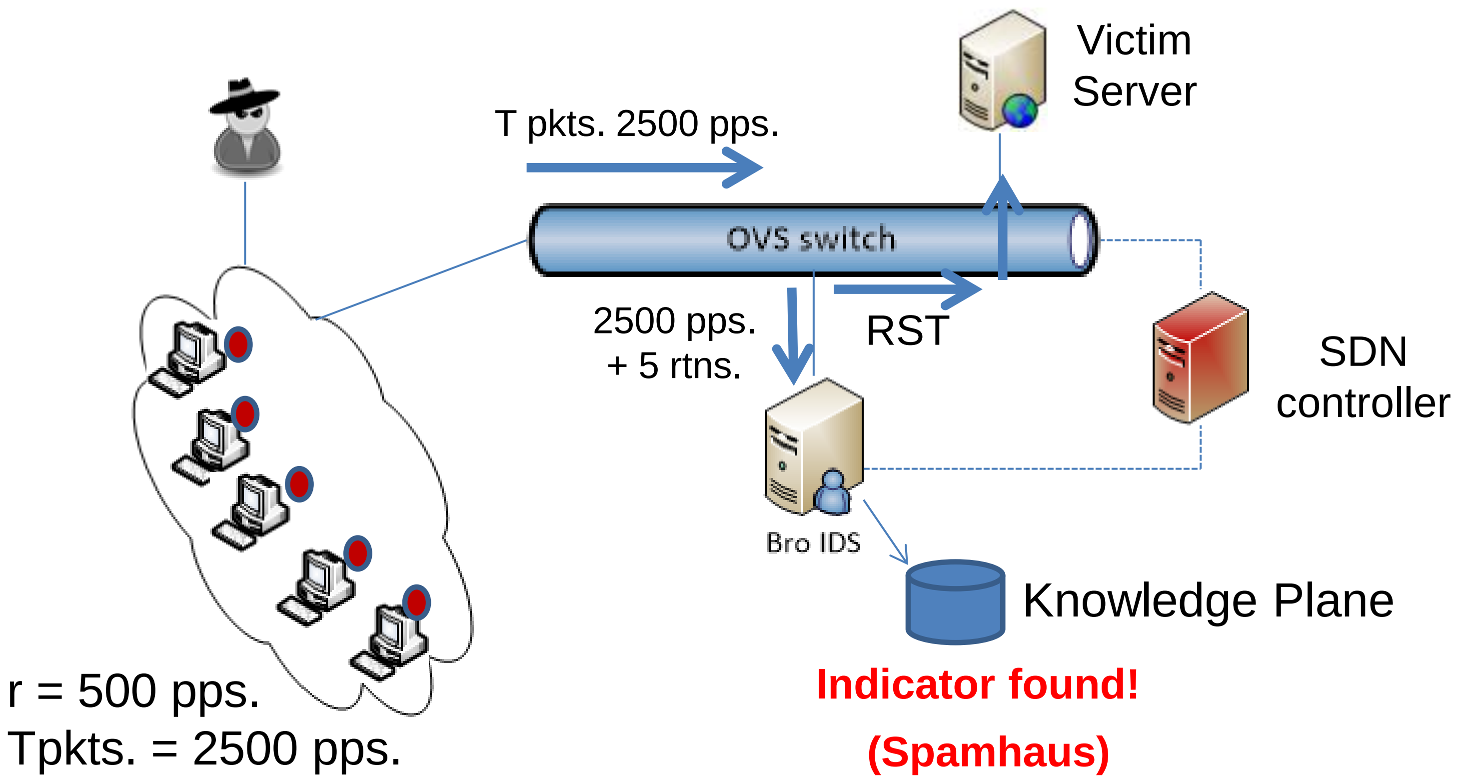
Methodology to counter password guessing-based attacks



5 malicious scanners scanning with TCP SYN or TCP ACK
With Intelligence: 1.8 seconds
Without Intelligence: Depending of the detection algorithm

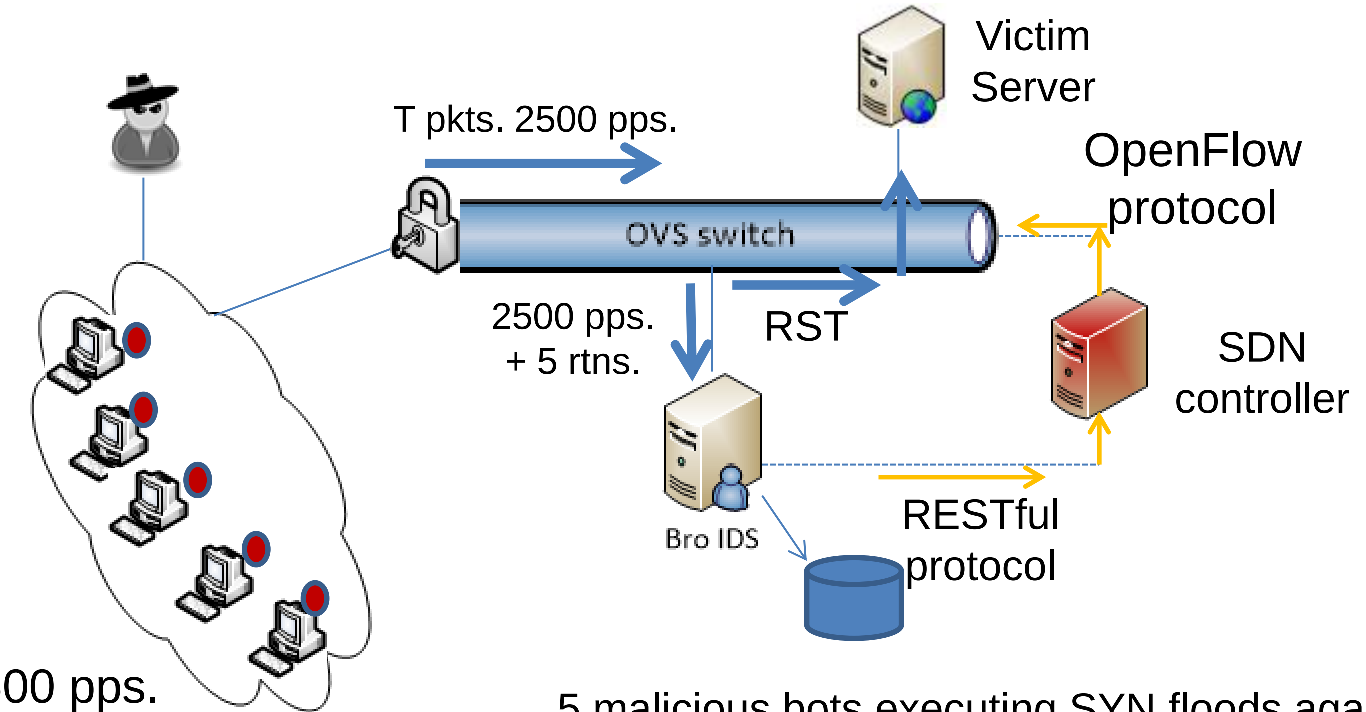
Experimental Evaluation 3

Methodology to counter password guessing-based attacks



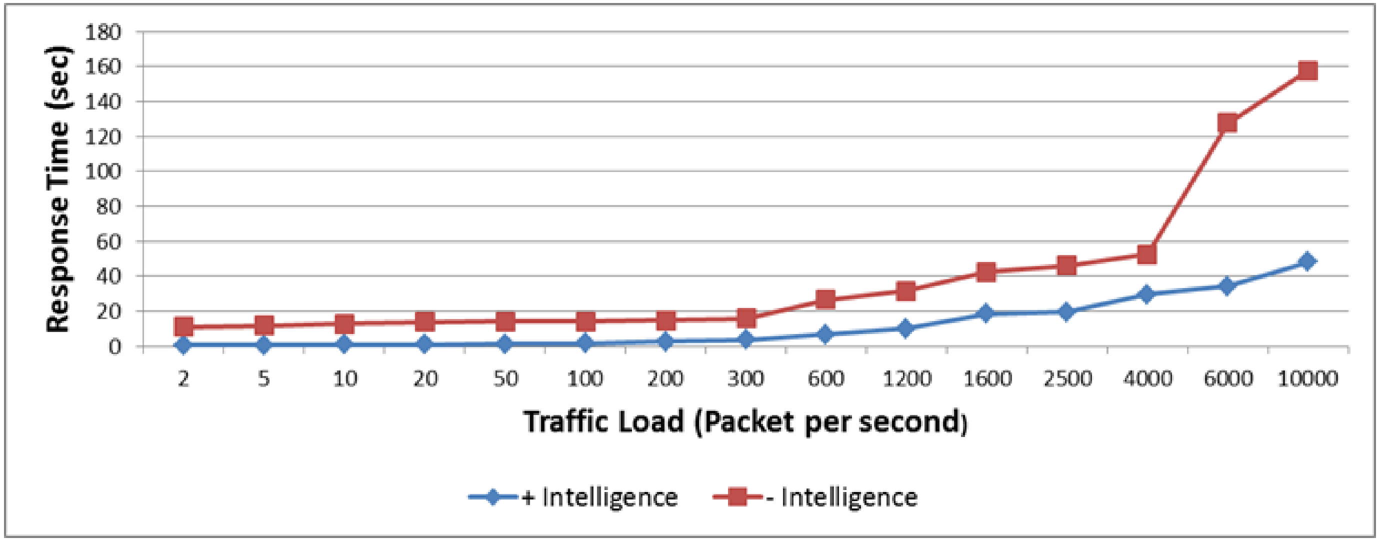
Experimental Evaluation 3

Methodology to counter password guessing-based attacks

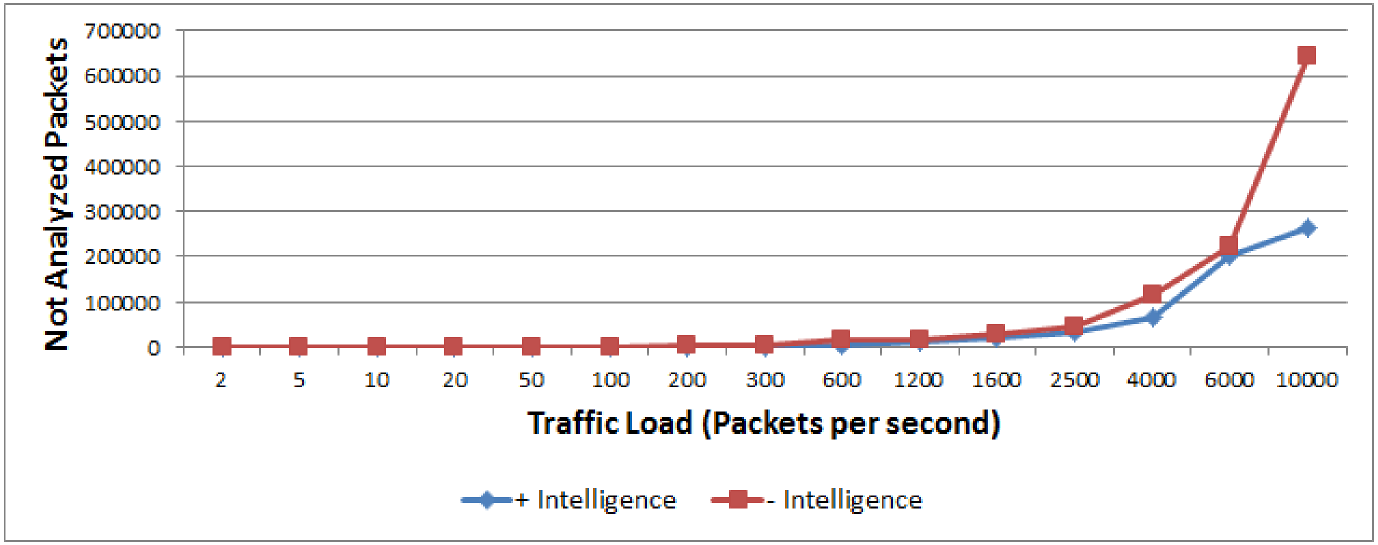


r = 500 pps.
Tpkts. = 2500 pps.

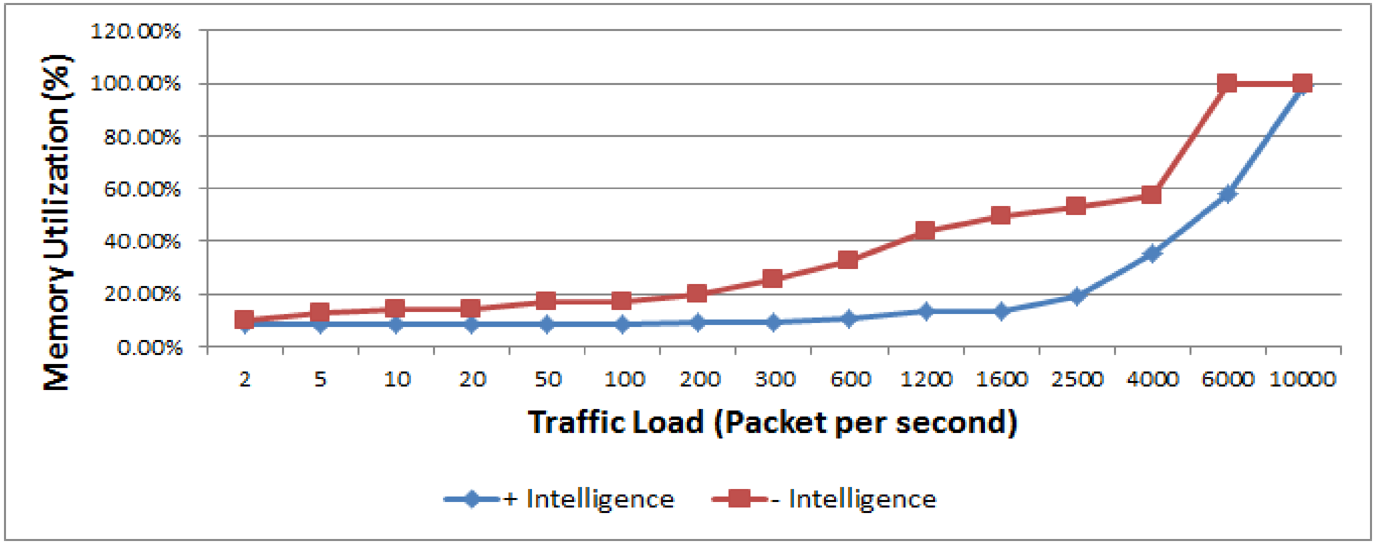
5 malicious bots executing SYN floods against a server
With Intelligence: 19.43 seconds
Without Intelligence: 46.21 seconds



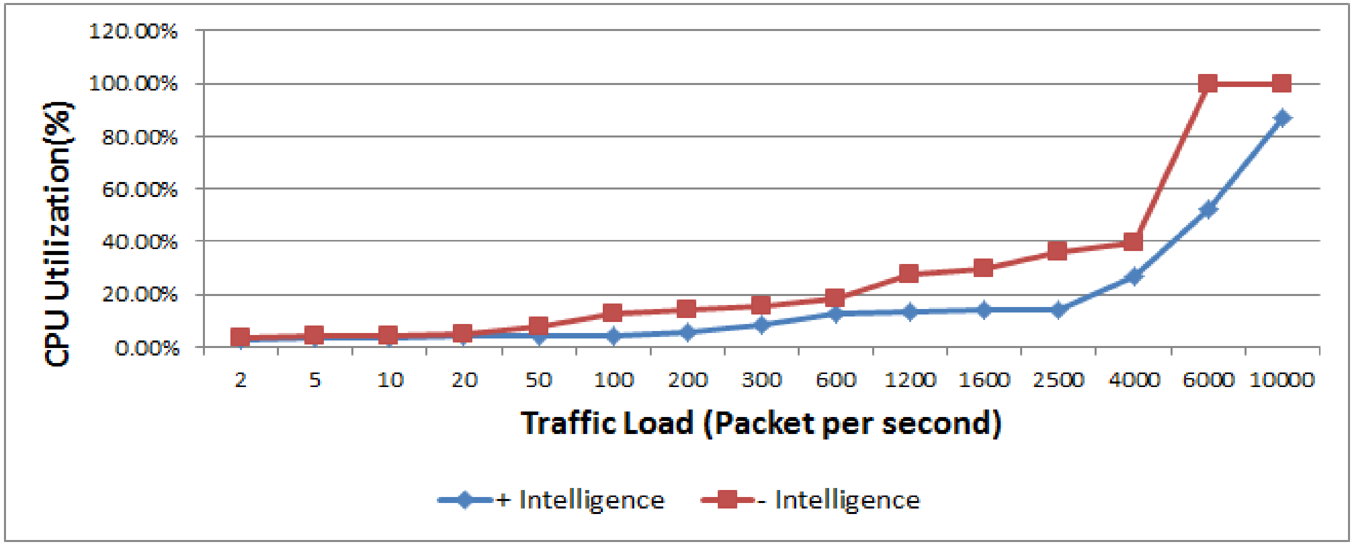
Comparison of the response time varying the rate of packet per second



Comparison of the unanalyzed packets varying the rate of packets per second



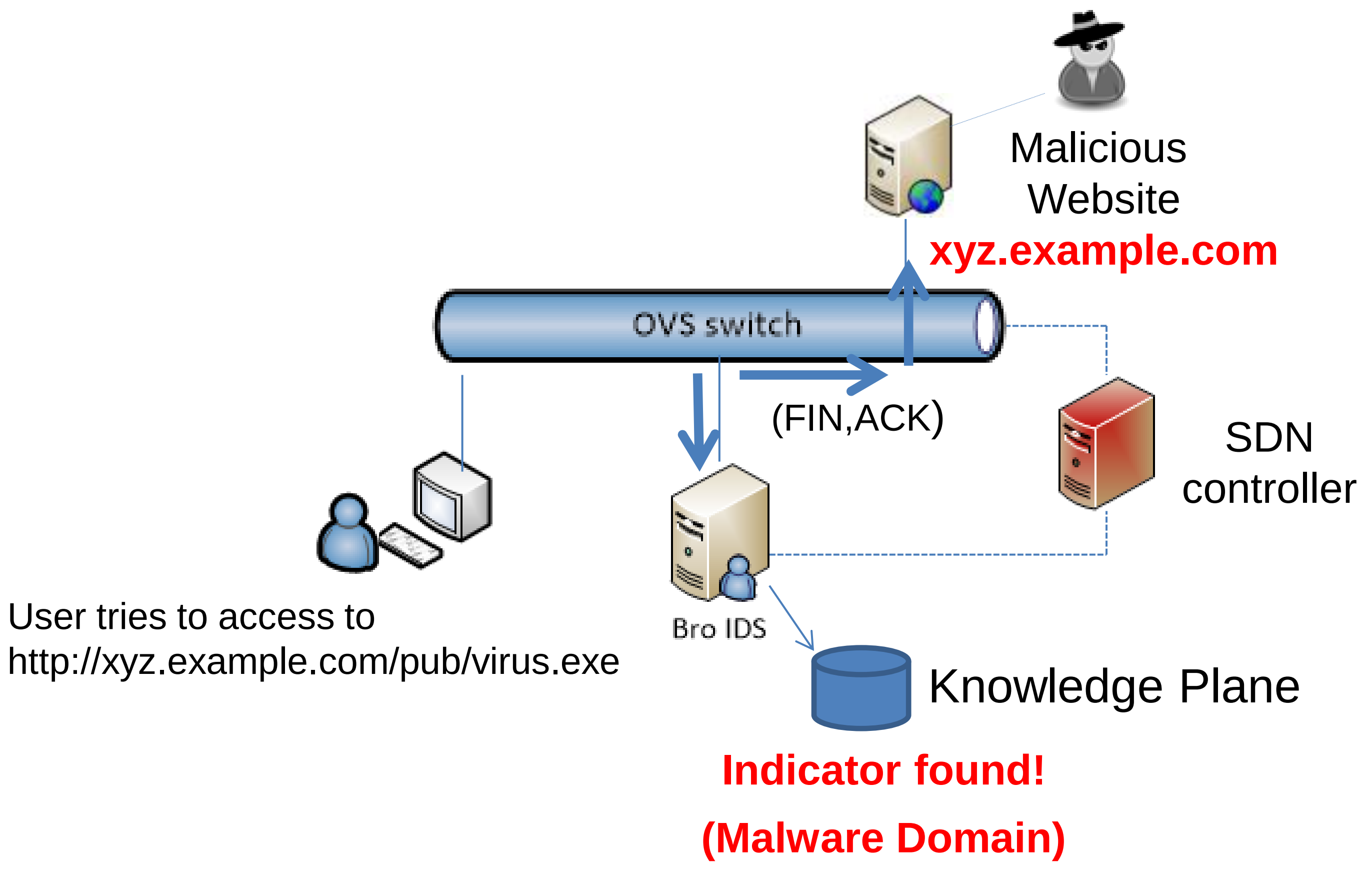
Comparison of the memory utilization performance varying the rate of packets per second



Comparison of the CPU utilization performance varying the rate of packets per second

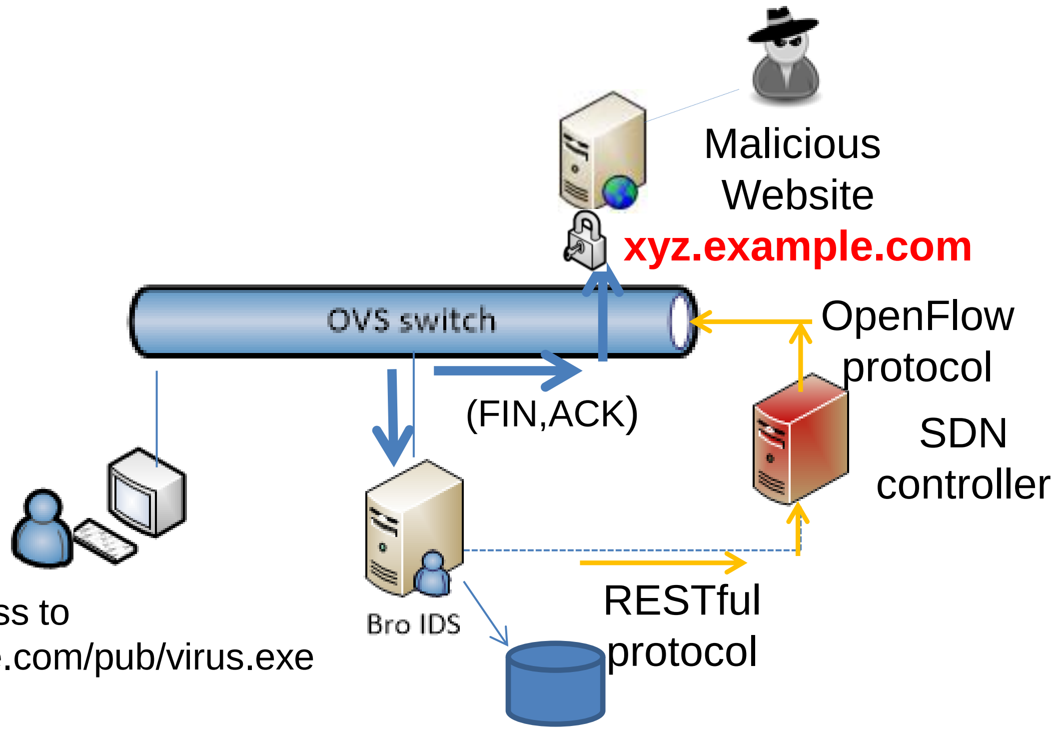
Experimental Evaluation 4

Methodology to counter password guessing-based attacks



Experimental Evaluation 4

Methodology to counter password guessing-based attacks



User tries to access to
http://xyz.example.com/pub/virus.exe

There are different malicious websites as well as malicious domains
With Intelligence: 0.07 seconds
Without Intelligence: No determined

Final Conclusions

- Malicious users are innovating their attacks techniques much faster than defenders have been findings ways to avoid them.
- The conventional approaches such as anomaly-based or signature-based detections are not enough to counter these new threats.
- Taking advantage of CTI, we can protect the network in less time that other proposals, by using Bro IDS intelligence framework and SDN.
- By using the proactive methodology, we update the KP each five minutes with intelligence provided by reliable organizations.
- Brute-force or dictionary attacks can be mitigated 100% using the intelligence, unlike the another methodology that only get mitigate less of 100%.

Final Conclusions

- Botnet attacks and port scanner get mitigated to 100% using the intelligence in better time that the another.
- Malicious website get mitigated in a time of 0.07 seconds for all cases.
- As future work, we pretend to explore with more detail the process of correlation of information obtained from reliable sources, and the statistics generated by using of OpenFlow, and by using the machine learning approach, we would generate security policies based on threats learned.

References

[Tianyi Xing 2013]

T. Xing, D. Huang, L. Xu, C.-J. Chung, and P. Khatkar, \Snortow: A openflow-based intrusion prevention system in cloud environment," in Proceedings of the 2013 Second GENI Research and Educational Experiment Workshop, GREE '13, (Washington, DC, USA), pp. 89{92, IEEE Computer Society, 2013.

[Tianyi Xing 2014]

T. Xing, Z. X., D. Huang, and D. M., \Sdnips: Enabling software-defined networking based intrusion prevention system in clouds," 10th International Conference on Network and Service Management, 2014.

[Martin Lopez 2014]

M. A. Lopez, U. Figueiredo, A. P. Lobato, and O. C. M. B. DUARTE, \Broflow: Um sistema eficiente de deteccao e prevencao de intrusao em redes definidas por software," in XXXIV Congresso da Sociedade Brasileira de Computacao { CSBC 2014, (Centro de Convencoes Brasil 21), CSBC2014, 2014.

References

[Antonio Lobato 2014]

A. P. Lobato, U. Figueiredo, M. A. Lopez, and O. C. M. B. DUARTE, Uma arquitetura elastica para prevencao de intrusao em redes virtuais usando redes definidas por software," in Anais do XXXII Simposio Brasileiro de Redes de Computadores e Sistemas Distribudos { SBRC 2014, (Florianopolis, SC, Brazil), SBRC 2014, 2014.

[Fábio Nagahama 2014]

F. Y. Nagahama, F. Farias, E. Aguiar, G. Luciano, L. Granville, E. Cerqueira, and A. Antonio, Ipsflow{uma proposta de sistema de prevencao de intrusao baseado no framework openflow," in III WPEIF-SBRC, vol. 12, pp. 42{47, 2012.

[Radware 2014]

RADWARE, \Defenseflow: The sdn application that programs networks for dos security," tech. rep., RADWARE.

References

List of Figures:

Source [1]: www.icp.ge.ch
Source [2]: blog.securestate.com
Source [3]: www.bro.org
Source [4]: www.isightpartners.com
Source [5]: clintonfirth.com
Source [6]: Article: “Software-Defined Networking: A Comprehensive Survey,” Proceeding of the IEEE
Source [7]: www.opennetworking.org

Thank you!
Questions?

Related Work

•**SnortFlow**: Proposes a flexible IPS system in cloud virtual networking environments, based on the performance evaluation of the virtual machines, reconfiguring the network in case of any abnormal activity [**Tianyi Xing 2013**].

•**BroFlow**: Proposes a system capable of reacting against DoS attacks in real time, combining an IDS and an OpenFlow application programming interface. BroFlow is an extension of the Bro architecture with two additional modules, one for the security policies and the other for message countermeasure. If there is a threat, a POX application either drops packets to eliminate malicious events or uses an output to forward packets to a specific target [**Martín Lopez 2014**].

•**Elastic Architecture for IPS**: Proposes methods to detect anomalies in an intra-domain network with multiples virtual networks and protection to the Deep Packet Inspection (DPI) monitoring tools as well a load balancing of the same, distributing flows in a suitable manner [**Antonio Lobato 2014**].

Related Work

•**IPSFlow**: Proposes a solution of IPS based on SDN/OpenFlow with automatized block of the malicious traffic. One of the advantages is the selective and distributed capture of the traffic in switches for the analyzing of one of more IDSs [**Fabio Nagahama 2012**].

•**Radware**: Provides a DDoS attack defense solution that leverages SDN technology taking actions of reconfiguration forwarding devices against DDoS attacks [**DefenseFlow 2013**]

•**SDNIPS**: Compares the SDN-based IPS solution with the traditional IPS approach from both mechanism analysis and evaluation. The network reconfiguration are designed and implemented based on POX controller to enhance its flexibility. Evaluations of SDNIPS demonstrated its feasibility and efficiency over traditional approaches [**Tianyi Xing 2014**].

Related Work

Name	Operation Mode	Inter domain	Controller	Countermeasure
SnortFlow [17]	Reactive	No	POX	Performance evaluation about SnortFlow agent deployed at Dom 0 is better than at Dom U for about 40 %
BroFlow [14]	Reactive	No	POX	Effective detecting DoS attacks caused by flooding and blocking attacks from its origin. Reducing delay at to 10 times on the networks under the attack and ensures the delivery of useful packets in the maximum rate of the link.
Elastic [16]	Reactive	No	POX	Blocking a malicious flow; evaluation of resources consumed for packet analysis and elasticity overload and discharge in Detecting Module intrusion.
IPSFlow [19]	Proactive	No	Undefined	Automatic blocks malicious traffic close to the orign
DefenseFlow [20]	Proactive	No	ODL, Cisco, etc	DDoS protection as a native network service and collect statistics
SciPass [23]	Reactive and Proactive	No	Owner	Improve transfer performance and reducing load on network infrastructure. Load balancing, bypass rules to avoid forwarding good data through firewalls of good data
IntelFlow	Reactive and Proactive	Yes	any	Detect and prevent certain threats on networks by a proactive mode and deploying countermeasures to the threats learned through the CTI which lead to the networking infrastructure layer being reconfigured through flow table updates to the data plane switches