Adapting Security Through Community Engagement

- Rajasekhar Ganduri
- Samuel Evans
- Logan Widick
- Mark Thompson
- Ram Dantu

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
College of Engineering
UNT®

Motivation

- Based on the growing number and severity of recent security breaches, security, as we know it, is failing!
  - Too vulnerable to the mistakes of individual programmers
  - Increasing size, number, and complexity of networks
  - Large attack surfaces, rushed deadlines
  - Continuously changing hardware, software, patches, …
- So, what's the net result?
  - Bear a mindset that security is too complex
  - Seem resigned to fact that security breaches are just a part of daily life
- But, security is everyone's responsibility!

Problem Approach

- So how can we fix this?
  1. Change the behavior of potential attackers
  2. Engage community of users to help solve the problem

- But if security professionals, who have been trained and certified to work on these systems, cannot fully secure these systems…
  – How can we expect an average person with little or no computer or security experience be expected to do so?

Community Engagement

- Security is only as good as its weakest link
  - Depends on human actions and knowledge
    - Best technologies in the world won’t work without the appropriate human behaviors/responses
  - And humans are the largest attack surface

- So why not leverage this to our advantage?
  - Extra eyes and ears on the problem
  - Everyone brings their own background and experience to the table

Who is Our Community?

- Consider the following setting
  - Business organization with WiFi network, such as a hotel
  - Cast of Characters
    - Trained security professional consultant
      - Consulted to configure network and security rules
    - Employees (manager, front desk, housekeeping, etc.)
      - Vested interest in organization
      - Typically technologically average
    - Customers
      - Users of WiFi network

Community Engagement

- So now we’re left with the question:

Can an average person with little or no computer or security experience effectively secure a system, such as a network?

  - Then, if not, how can we get there?

- Approach from two different perspectives
  1. User education and training
  2. Natural language enabled technology interface
     a. Data Collection: Can average individuals engage with a network security appliance?
     b. Data Translation: Can the network security appliance translate natural language correctly and effectively?

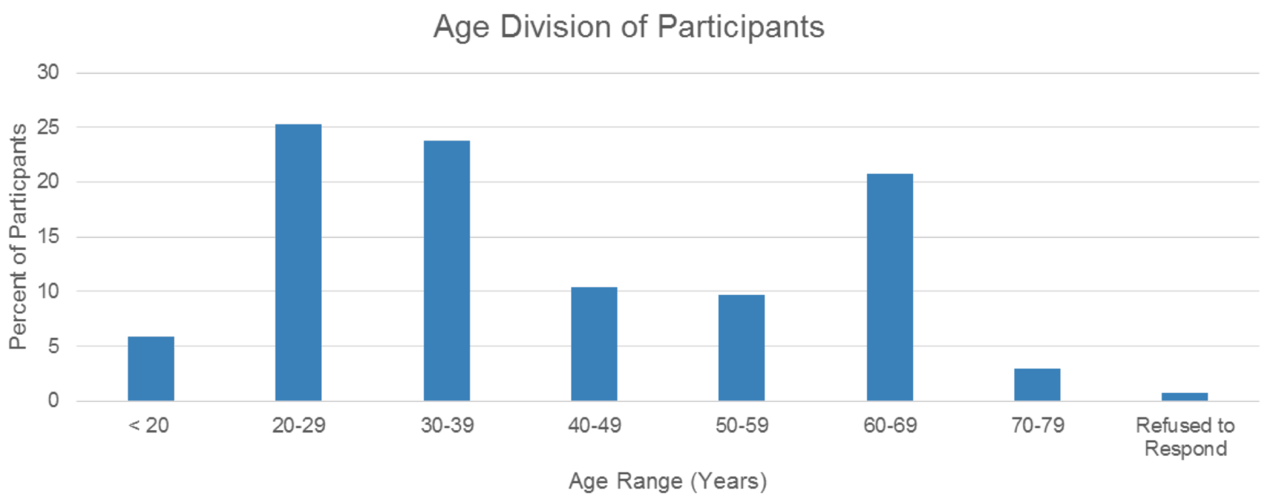
Data Collection

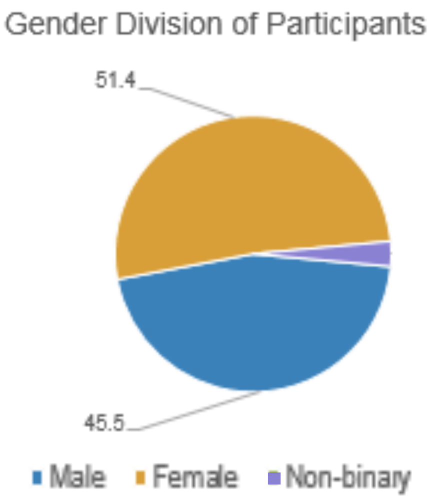
Can average individuals engage with a network security appliance?

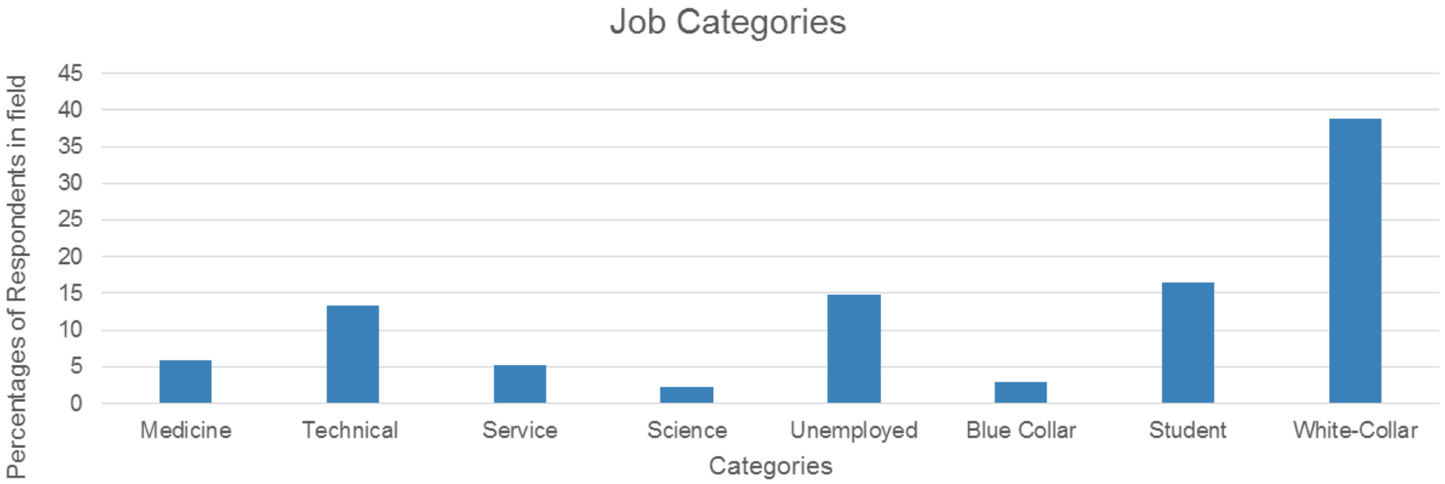
Natural Language Processing

- Can natural language processing be used to enable technologically average individuals to engage meaningfully and effectively with network security appliances?
  - Need ascertain if can address certain kinds of network-related problems that the end-system can deal with
  - Survey
    - Participants had to phrase how to give orders to another human being capable of instituting network changes that they needed

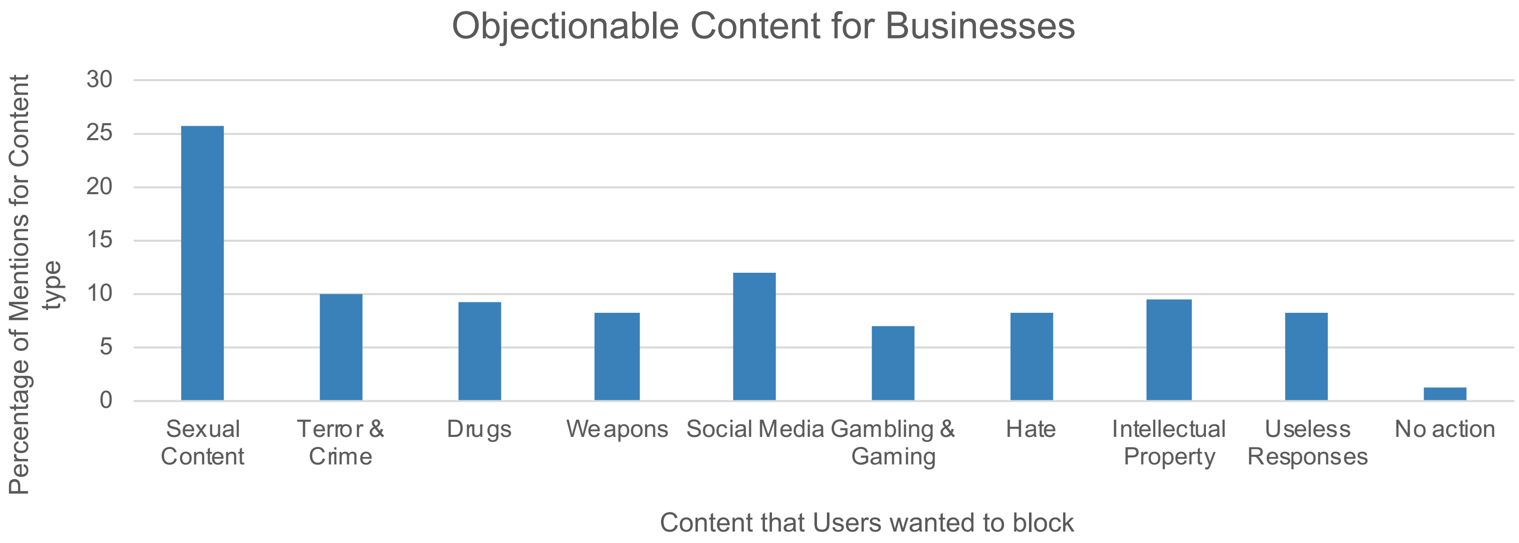
Participant Demographics


Age Division of Participants


Gender Division of Participants

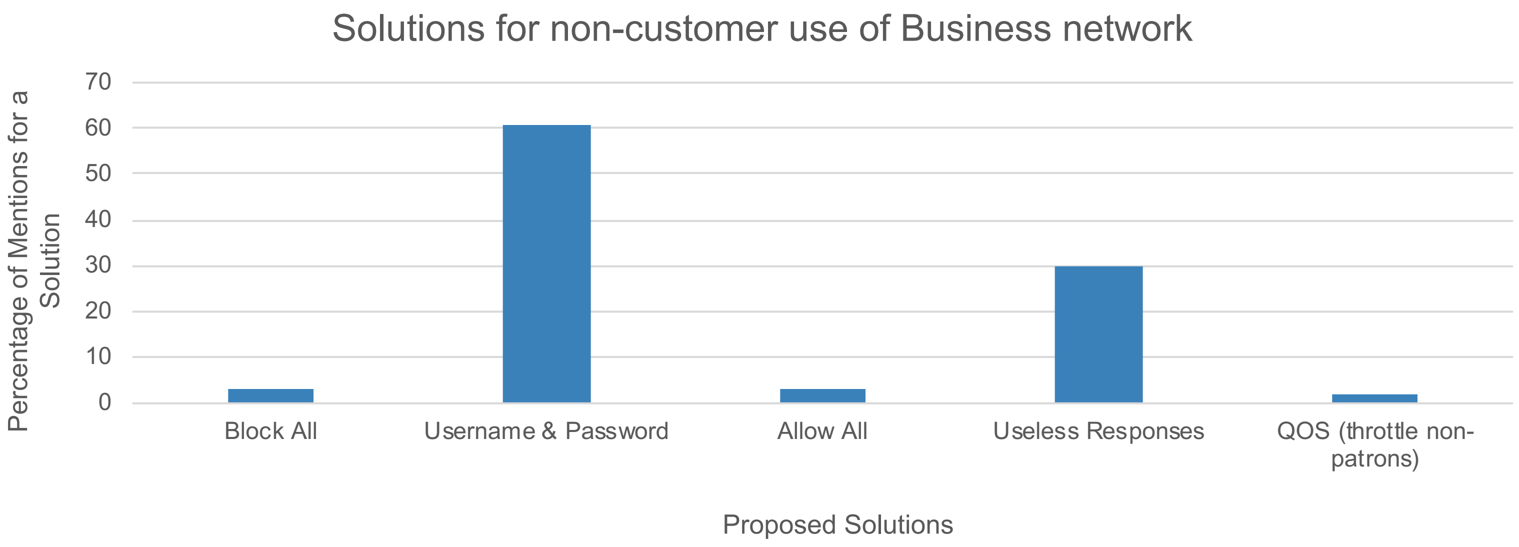

Job Categories

Identify Objectionable Content



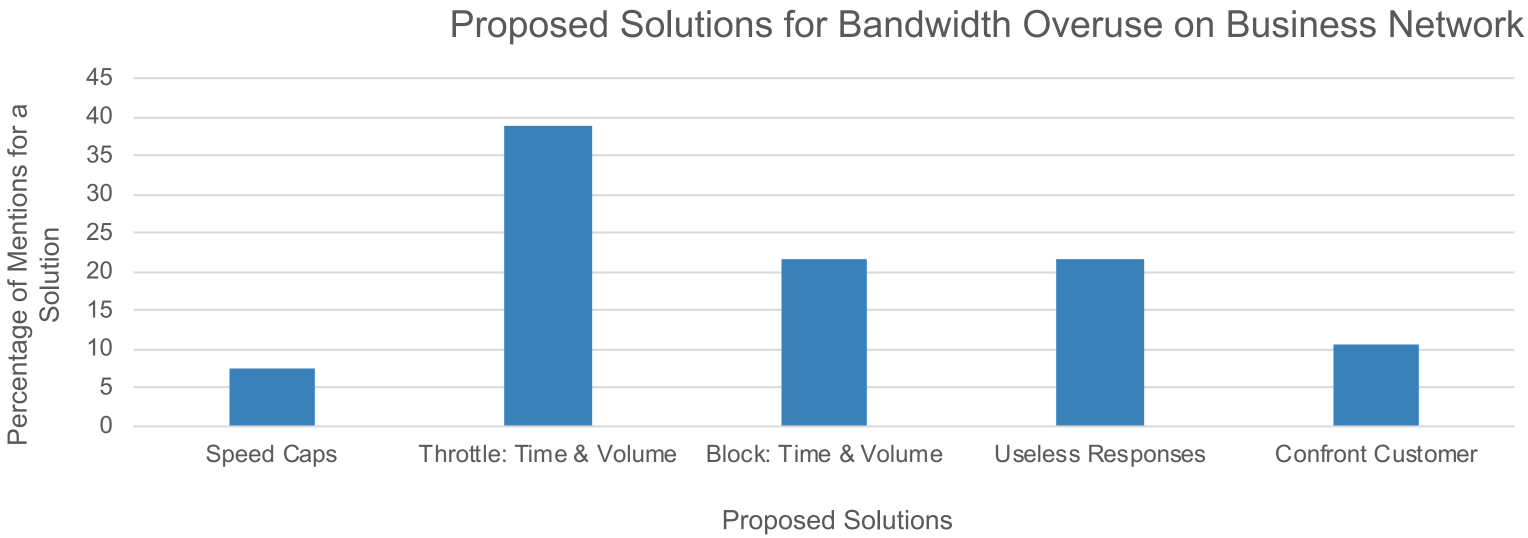
- Can participants identify objectionable content?
  - "Not Safe for Work" topics
  - "Useless Responses" did not address the question

Prevent Unwanted Network Use



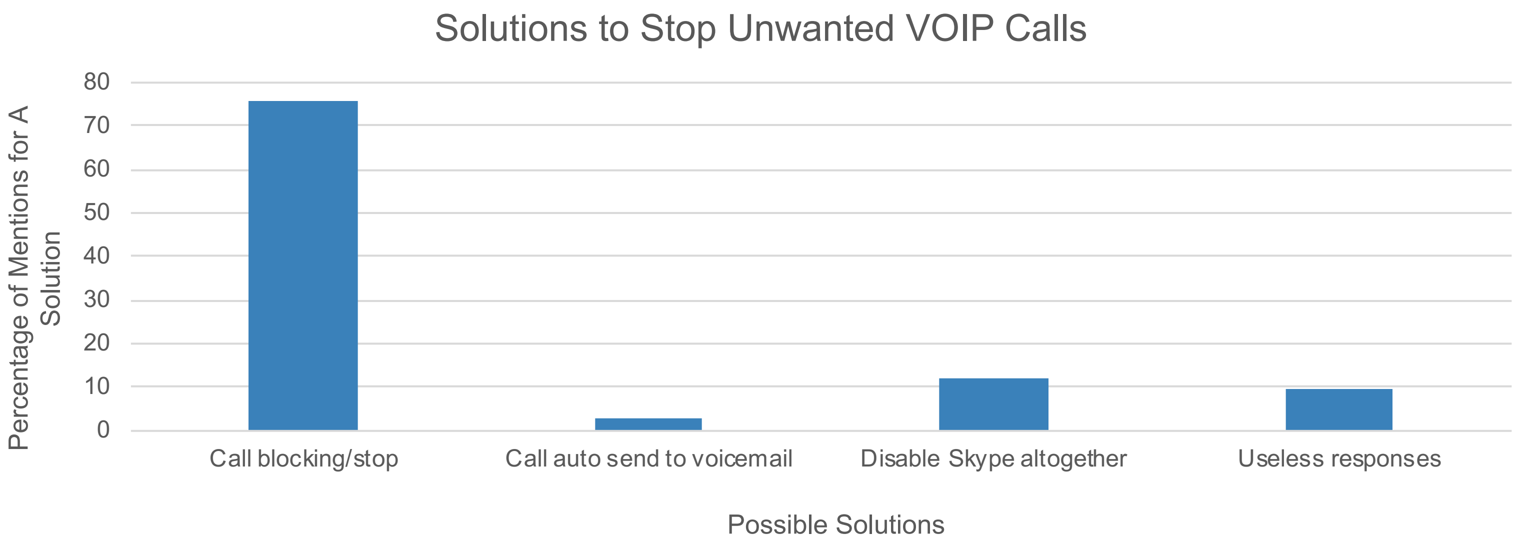
- How would participants prevent unwanted network use?
  - – "Useless Responses" did not address the question or did not know how to answer
    - High number indicates user training/education needed

Prevent Bandwidth Network Overuse



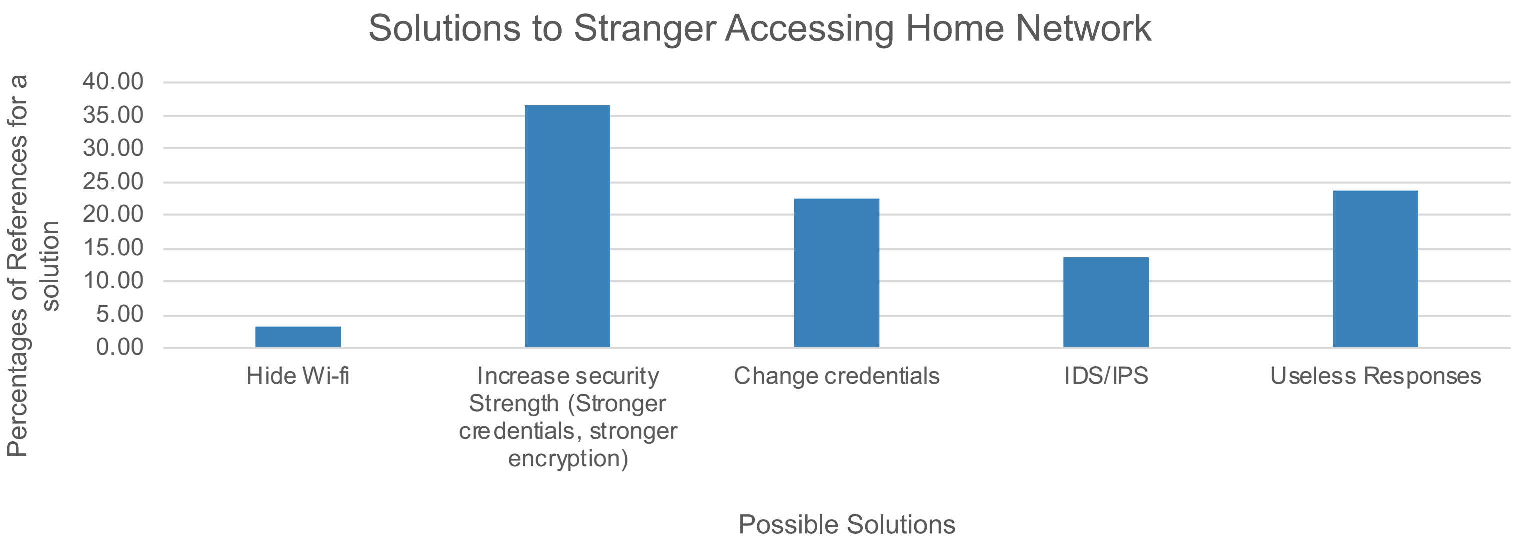
- How would participants prevent a user consuming significant bandwidth on the network?
  - "Useless Responses" did not address the question or did not know how to answer
    - High number indicates help from NLP system needed

Prevent Spam VoIP Calls



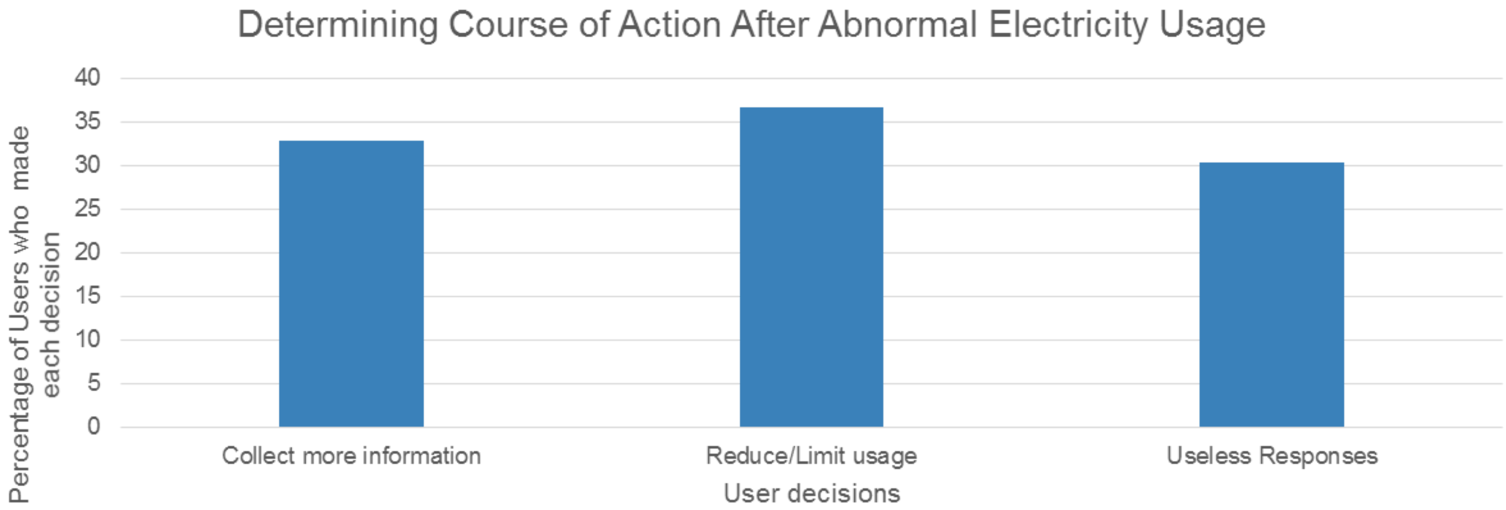
- How would participants prevent receiving a disruptive number of calls over a VoIP service?
  - Most chose to block relevant numbers, but some chose to disable service altogether

Prevent Unwanted Network Access



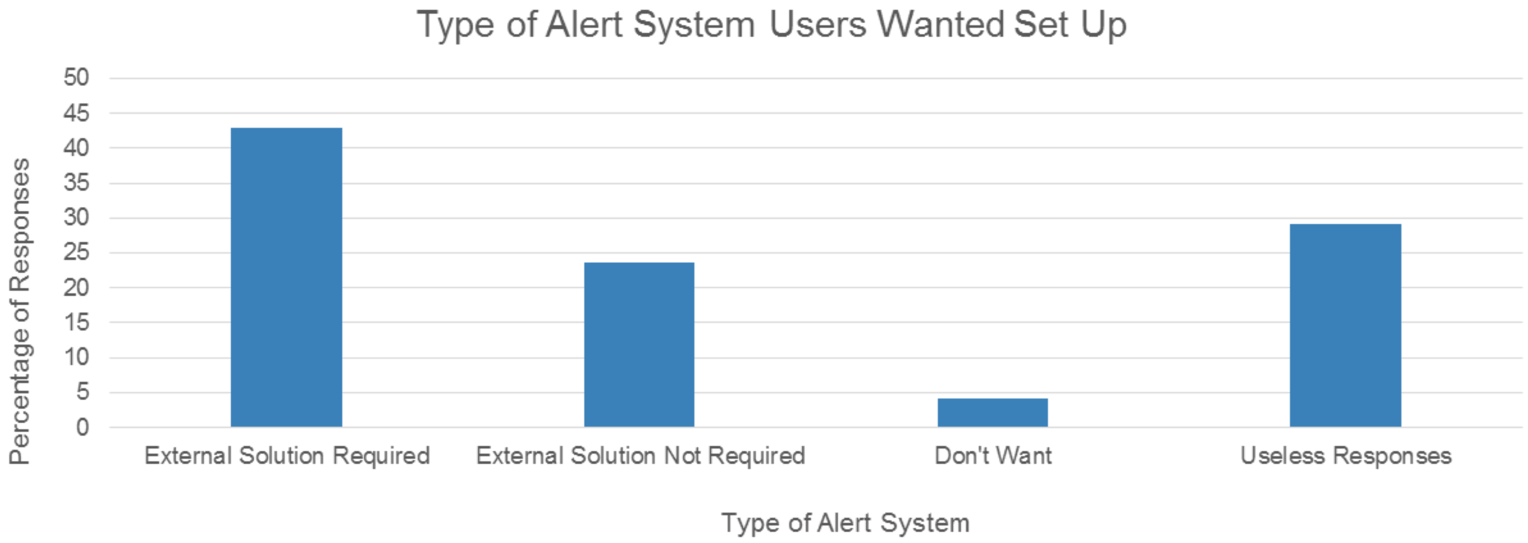
- How would participants prevent an unknown user attempting to access their home network?
  - Most suggested investment in stronger security
    - Some suggested solutions for preventing intrusions that could be implemented with an IDS or IPS

Determine Course of Action



- What course of action would participants take when their utility bill indicates someone is using substantial amount of electricity at night?
  - – Restrict by time-of-day or use Internet to prevent activity
  - – Investigate more deeply to determine exact cause of usage

Set Up an Alert System



- How would participants set up a system that monitored for danger (network-based or physical) and alert themselves and a trusted neighbor when danger occurred?
  - "External Solution Required" denotes solution requires additional input from devices (e.g., sensors, cameras, etc.)
  - High number of "Useless Responses"

Data Translation

Can the network security appliance translate natural language correctly and effectively?

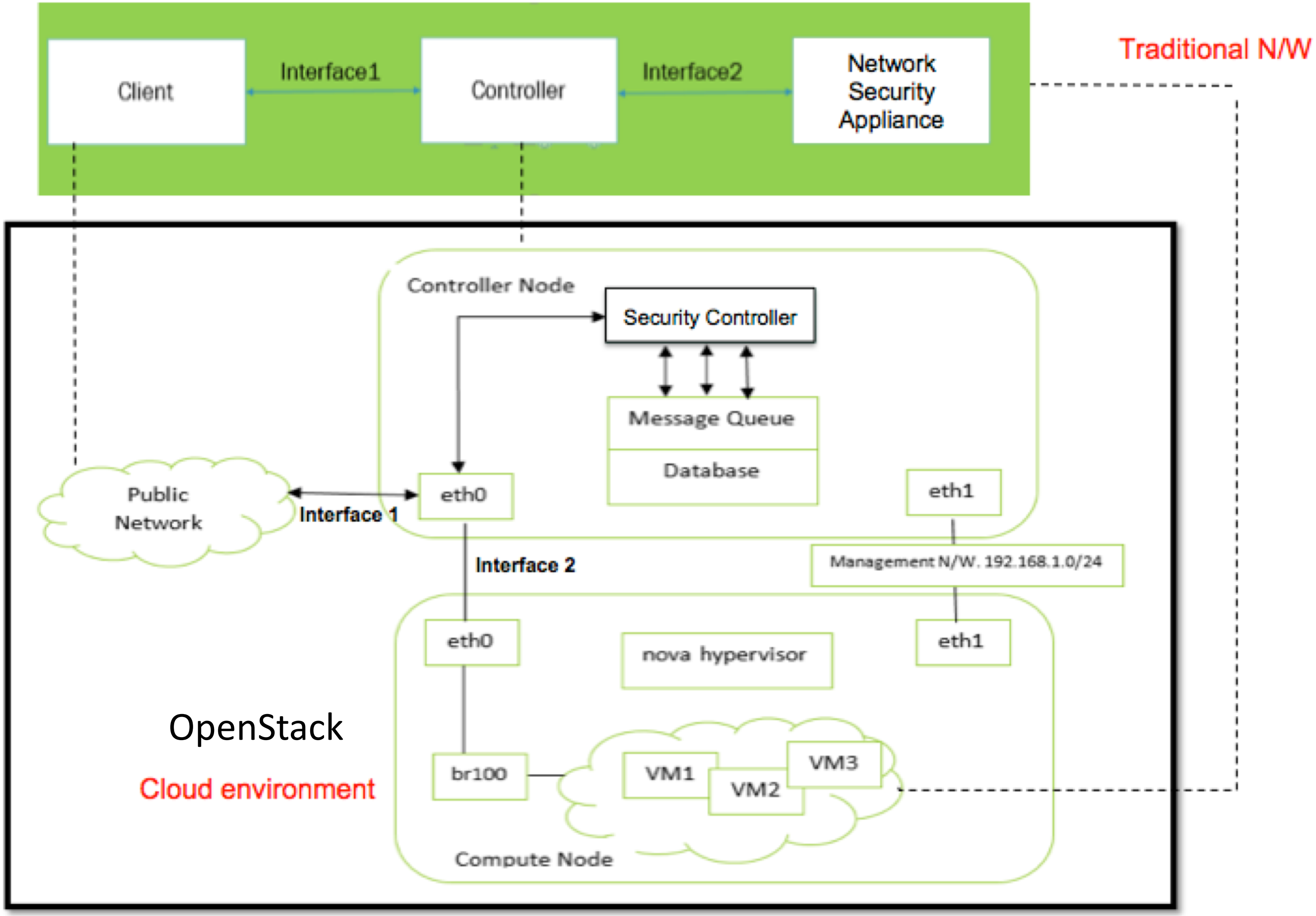
Security Controller

- Function as main point of contact between client and network security appliances
  - Implemented within open source, virtualized private cloud environment called OpenStack

Phases

  - Interpretation
    - Check grammar, semantics and validate
    - Detect keywords for network security appliance (firewall, IDS)
    - Translate to intermediate string with appliance detected
  - Translation
    - Detect important information
    - Construct the network security appliance rule
  - Installation
    - Transfer the output files
    - Execute the network security appliances with new rules

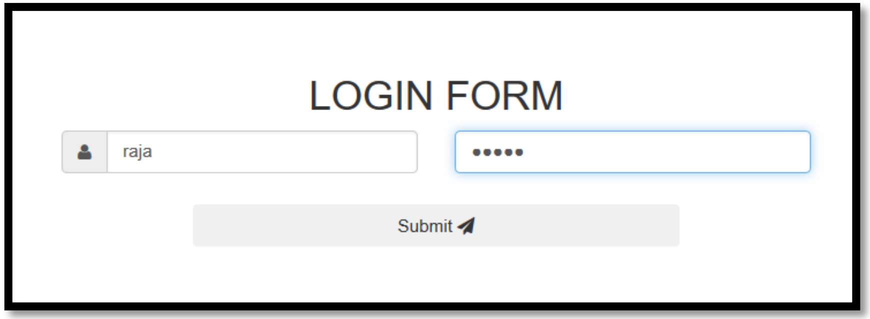
Deployment Architecture



Network Security Appliances

- Snort IDS
  - Network Intrusion Detection System (IDS)
  - Signature-Based
- Cisco FWSM – Network-Based Firewall
  - Stateful Firewall
  - Transparent or Stealth Mode
- Netfilter – Host-Based Firewall
  - Packet Filtering and NAT Rules

Client Interface



LOGIN FORM

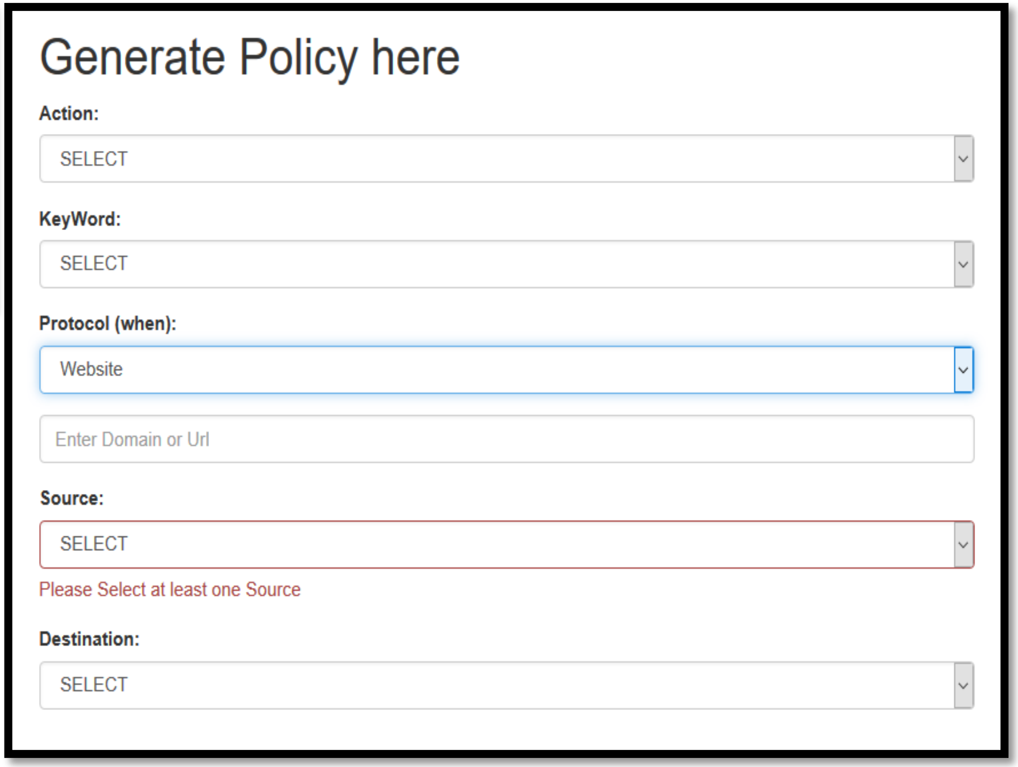
raja

•••••

Submit

Access Control

- Displayed fields depend on the user's role
- Policies can be entered through drop-down lists or a text box



Generate Policy here

Action: SELECT

KeyWord: SELECT

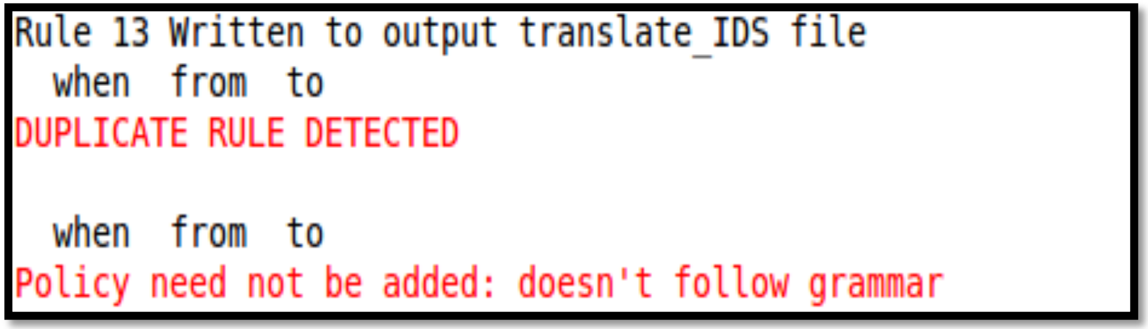
Protocol (when): Website

Enter Domain or Url

Source: SELECT

Please Select at least one Source

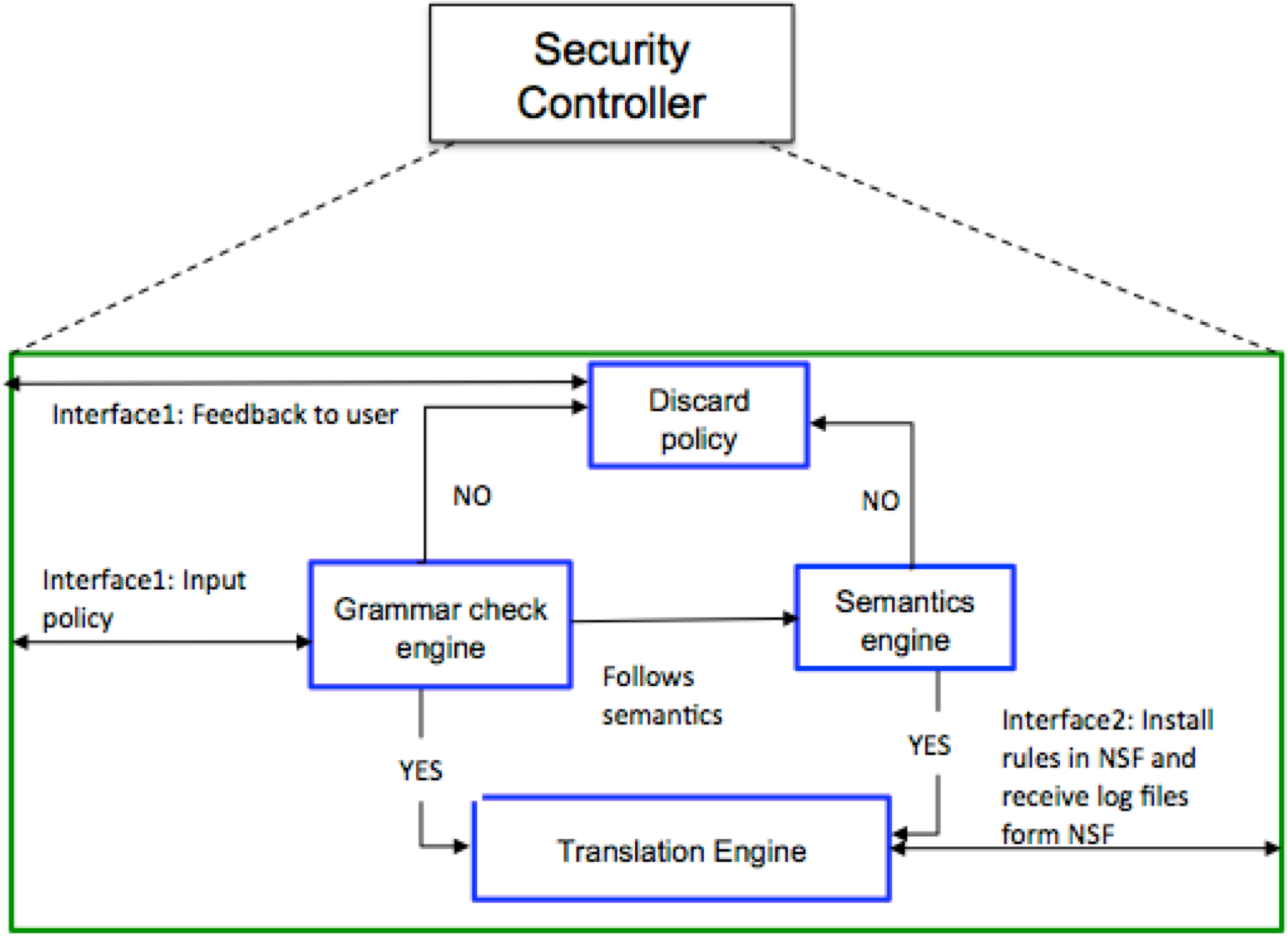
Destination: SELECT



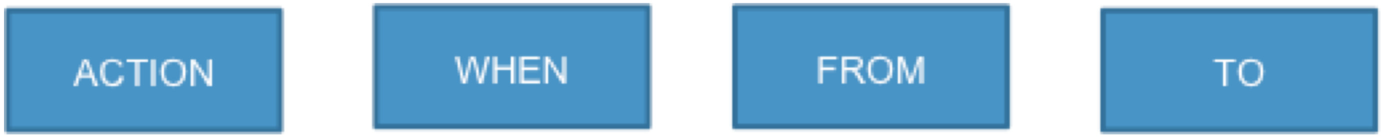
```
Rule 13 Written to output translate_IDS file
  when  from  to
DUPLICATE RULE DETECTED

  when  from  to
Policy need not be added: doesn't follow grammar
```

- User can view generated policy
- Receive feedback on input policies

Security Controller Architecture



Grammar Engine



ACTION WHEN FROM TO

Snort IDS

- alert
- log
- activate
- dynamic
- pass

Firewall

- allow
- accept
- permit
- deny
- block
- reject

Protocols

- tcp
- http
- https
- ftp
- icmp
- udp
- …

Source and Destination Machines

- external network
- home network
- subnet1
- network security appliances
- workstations/VMs in a network
- …

Example

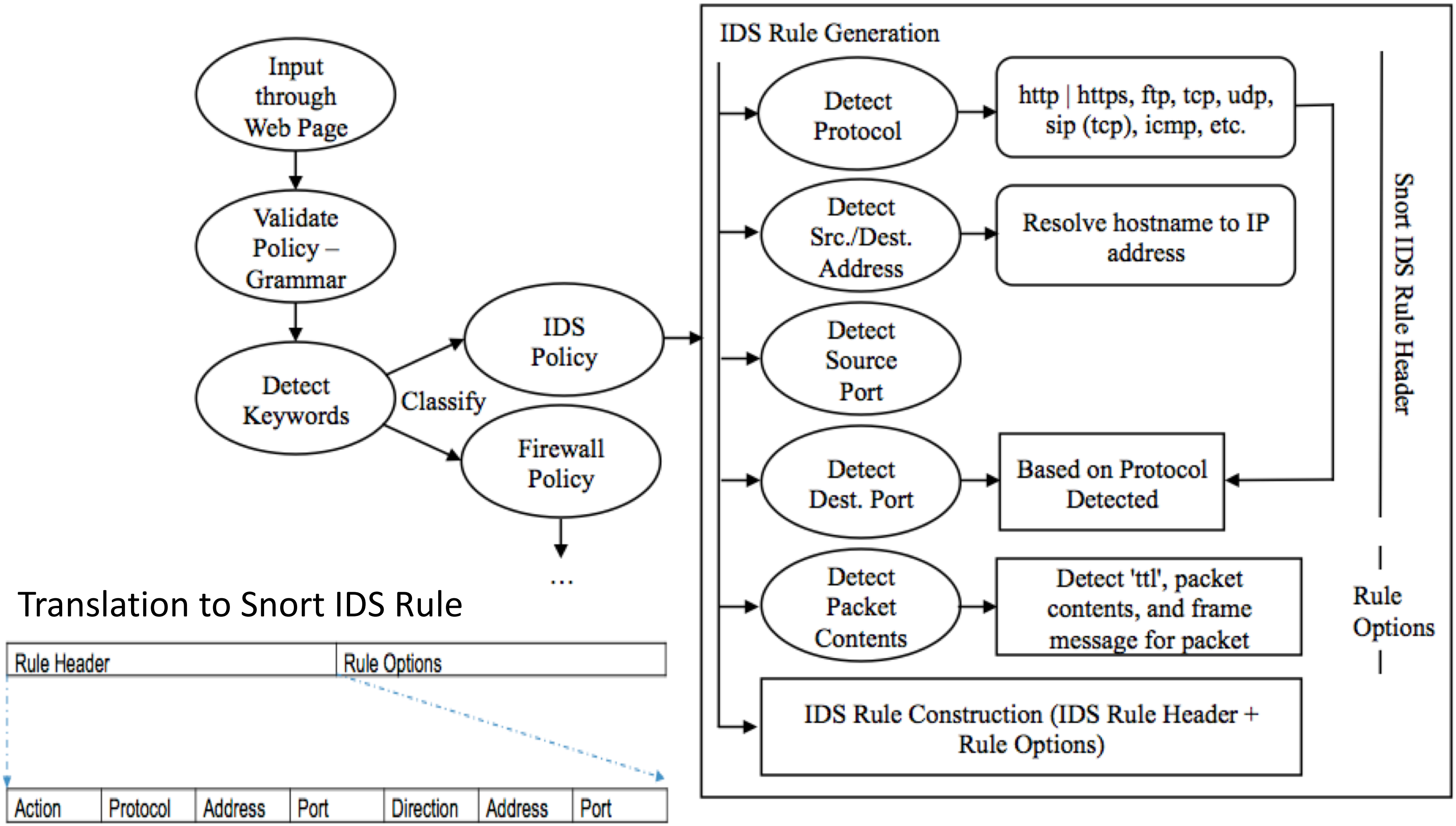
"alert when ping from PC1 to PC2"

Semantics Engine

- The semantics engine checks for the validity and logic of the input policy

alert when ping from PC1 to PC2	Grammatically correct
- - OR - -	
alert when PC1 pings PC2	Semantically correct
block ssh from subnet1 firewall to PC1	Semantically incorrect

Translation to Snort IDS Rule

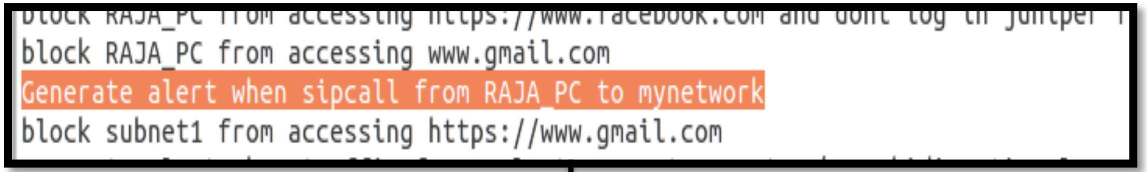

Input through Web Page
Validate Policy – Grammar
Detect Keywords
Classify
IDS Policy
Firewall Policy
…
IDS Rule Generation
Detect Protocol
http | https, ftp, tcp, udp, sip (tcp), icmp, etc.
Detect Src./Dest. Address
Resolve hostname to IP address
Detect Source Port
Detect Dest. Port
Based on Protocol Detected
Detect Packet Contents
Detect 'ttl', packet contents, and frame message for packet
IDS Rule Construction (IDS Rule Header + Rule Options)
Snort IDS Rule Header
Rule Options

Translation to Snort IDS Rule

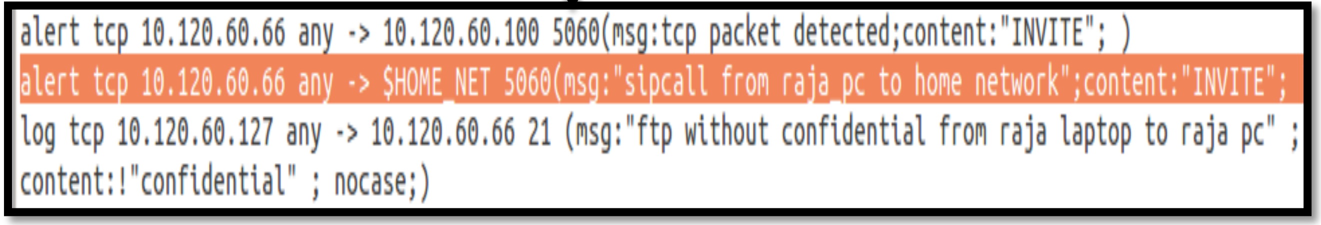
Rule Header	Rule Options

Action	Protocol	Address	Port	Direction	Address	Port

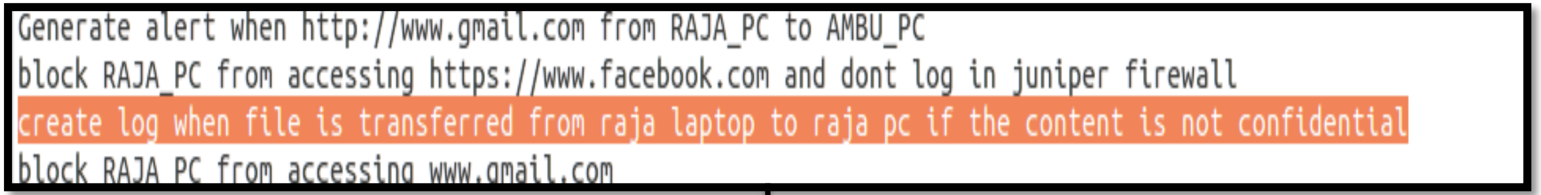
Snort IDS Rule Examples



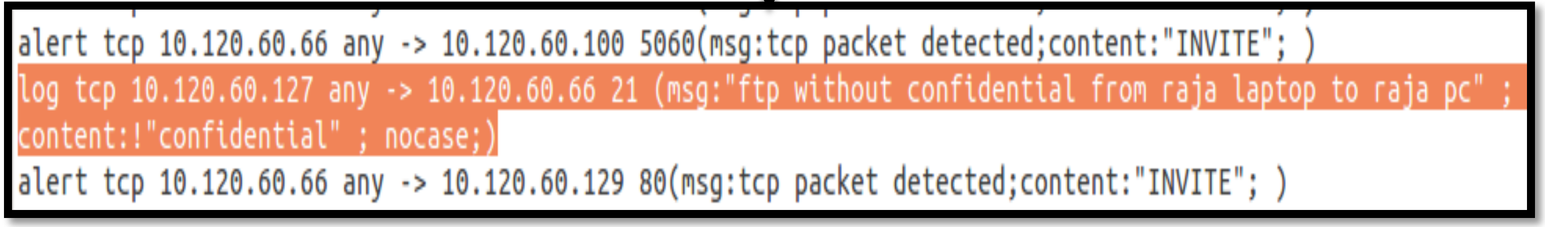
```
block RAJA_PC from accessing https://www.facebook.com and dont log in juniper f
block RAJA_PC from accessing www.gmail.com
Generate alert when sipcall from RAJA_PC to mynetwork
block subnet1 from accessing https://www.gmail.com
```



```
alert tcp 10.120.60.66 any -> 10.120.60.100 5060(msg:tcp packet detected;content:"INVITE"; )
alert tcp 10.120.60.66 any -> $HOME_NET 5060(msg:"sipcall from raja_pc to home network";content:"INVITE";
log tcp 10.120.60.127 any -> 10.120.60.66 21 (msg:"ftp without confidential from raja laptop to raja pc" ;
content:!"confidential" ; nocase;)
```



```
Generate alert when http://www.gmail.com from RAJA_PC to AMBU_PC
block RAJA_PC from accessing https://www.facebook.com and dont log in juniper firewall
create log when file is transferred from raja laptop to raja pc if the content is not confidential
block RAJA_PC from accessing www.gmail.com
```

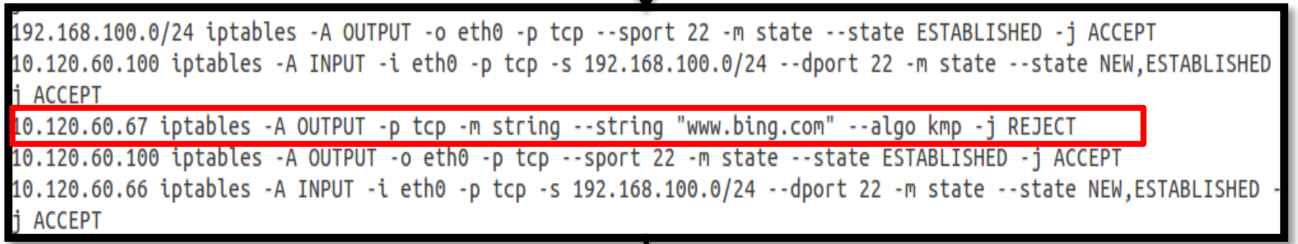


```
alert tcp 10.120.60.66 any -> 10.120.60.100 5060(msg:tcp packet detected;content:"INVITE"; )
log tcp 10.120.60.127 any -> 10.120.60.66 21 (msg:"ftp without confidential from raja laptop to raja pc" ;
content:!"confidential" ; nocase;)
alert tcp 10.120.60.66 any -> 10.120.60.129 80(msg:tcp packet detected;content:"INVITE"; )
```

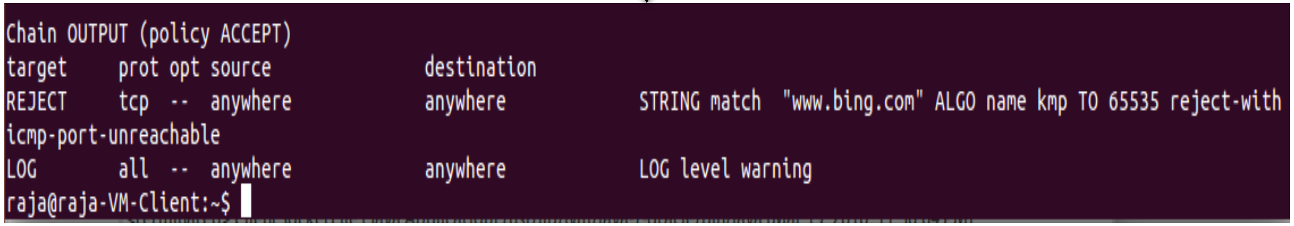
Translation to iptables Rules

iptables	option	chain	matching criteria	target

"block www.bing.com to hostA"



```
192.168.100.0/24 iptables -A OUTPUT -o eth0 -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT
10.120.60.100 iptables -A INPUT -i eth0 -p tcp -s 192.168.100.0/24 --dport 22 -m state --state NEW,ESTABLISHED
j ACCEPT
10.120.60.67 iptables -A OUTPUT -p tcp -m string --string "www.bing.com" --algo kmp -j REJECT
10.120.60.100 iptables -A OUTPUT -o eth0 -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT
10.120.60.66 iptables -A INPUT -i eth0 -p tcp -s 192.168.100.0/24 --dport 22 -m state --state NEW,ESTABLISHED -
j ACCEPT
```



```
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
REJECT     tcp  --  anywhere             anywhere             STRING match  "www.bing.com" ALGO name kmp TO 65535 reject-with
icmp-port-unreachable
LOG        all  --  anywhere             anywhere             LOG level warning
raja@raja-VM-Client:~$ 
```

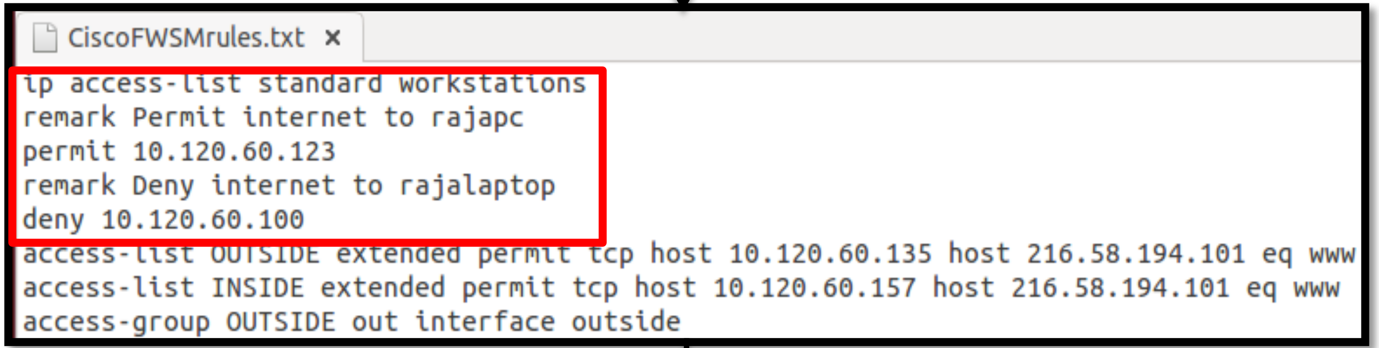
Translation to Cisco FWSM Rules

access-list <direction of traffic> extended <action to be taken> <protocol> <src ip> <dst ip>

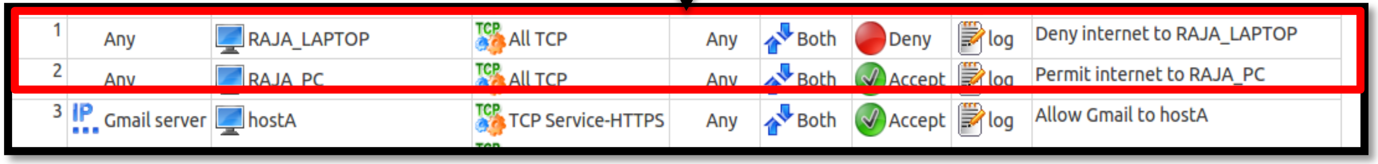
access-group <traffic direction> direction interface <interface name>

"Allow internet to rajapc"

"Deny internet to rajalaptop"



```
ip access-list standard workstations
remark Permit internet to rajapc
permit 10.120.60.123
remark Deny internet to rajalaptop
deny 10.120.60.100
access-list OUTSIDE extended permit tcp host 10.120.60.135 host 216.58.194.101 eq www
access-list INSIDE extended permit tcp host 10.120.60.157 host 216.58.194.101 eq www
access-group OUTSIDE out interface outside
```

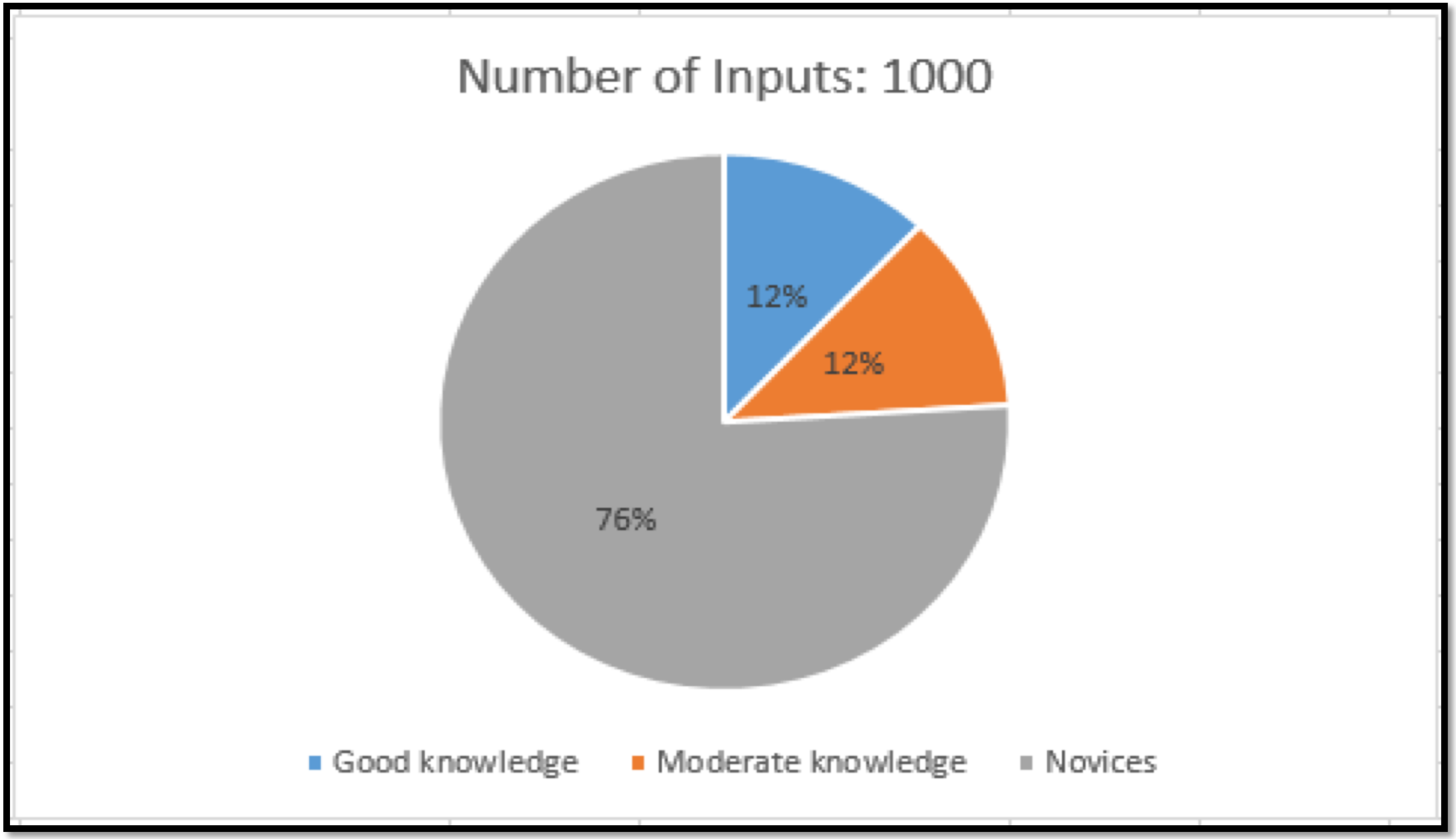


1	Any	RAJA_LAPTOP	All TCP	Any	Both	Deny	log	Deny internet to RAJA_LAPTOP
2	Any	RAJA_PC	All TCP	Any	Both	Accept	log	Permit internet to RAJA_PC
3	Gmail server	hostA	TCP Service-HTTPS	Any	Both	Accept	log	Allow Gmail to hostA

Testing and Performance

Results and Conclusion

User Experience Level

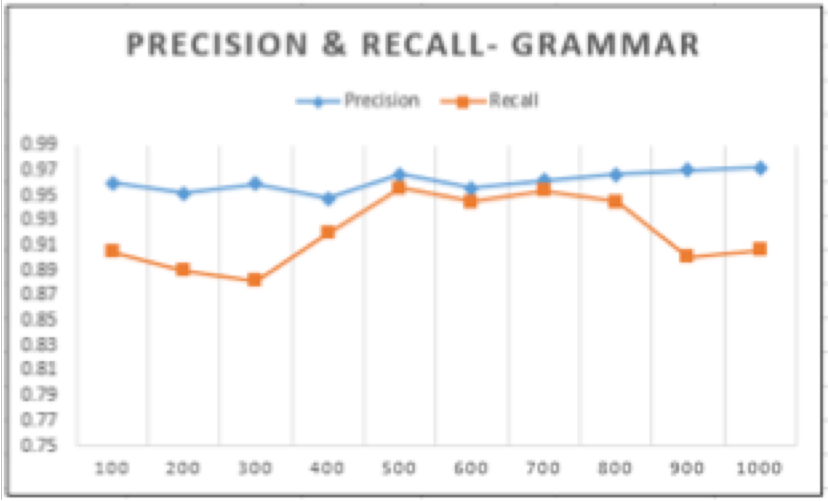


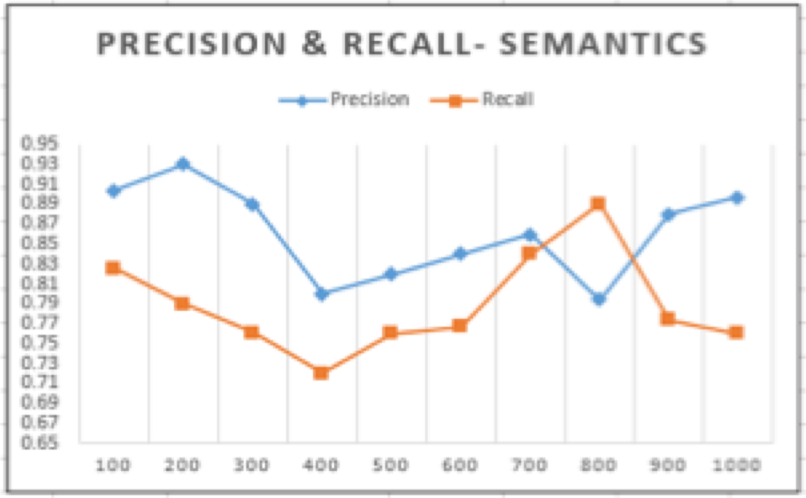
Performance Analysis

- Interpretation
  - Accuracy
  - Precision
  - Recall
  - F1 Score
- Translation
  - Similarity of Generated Rule with Standard Rule
    - Levenshtein Distance, Cosine Similarity
- Installation
  - Acceptance and Rejection Rates by Network Security Appliances

Precision and Recall

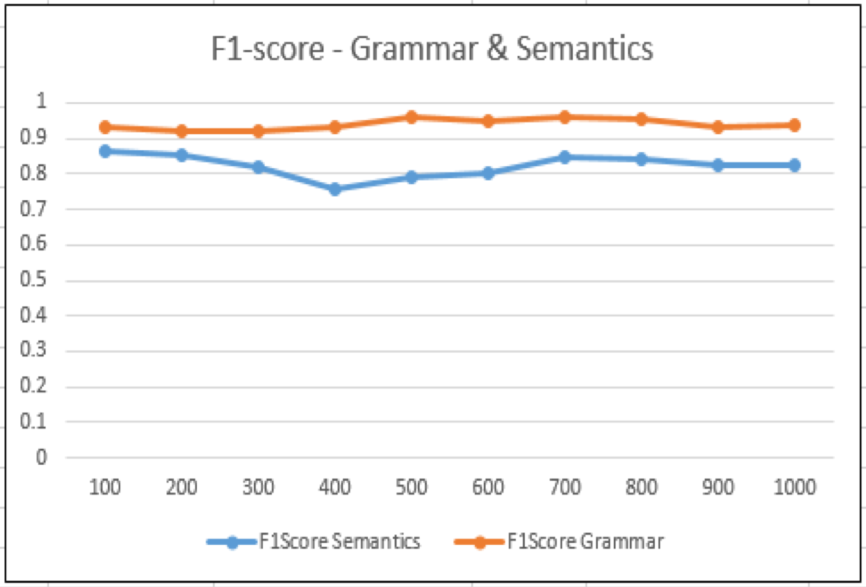
- Precision: The number of correctly interpreted policies by total number of all interpreted policies
- Recall: The number of correctly interpreted policies by total number of interpreted policies that are supposed to be correct

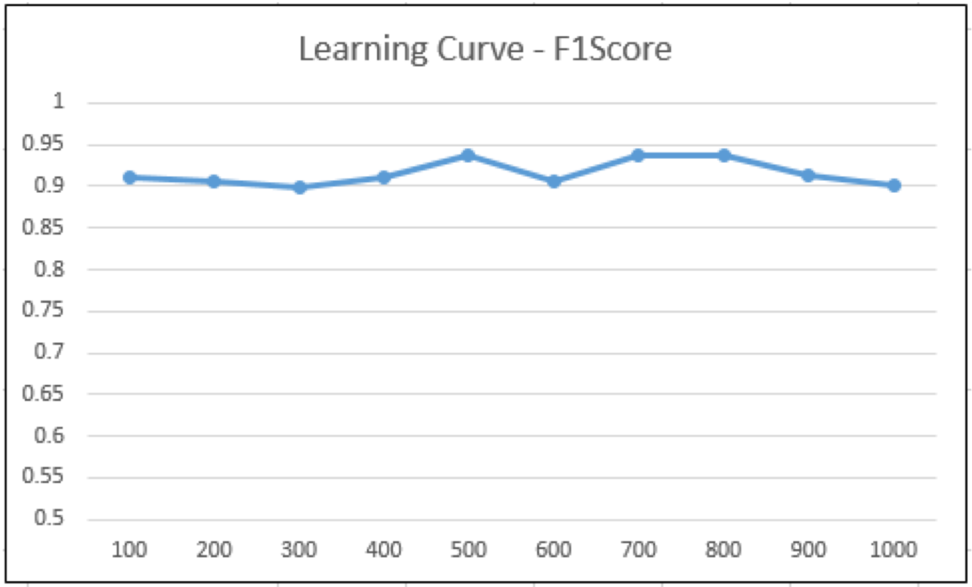




- Recall rate of semantics engine is relatively lower (0.76) due to higher false negative rate in semantics engine

F1 Score

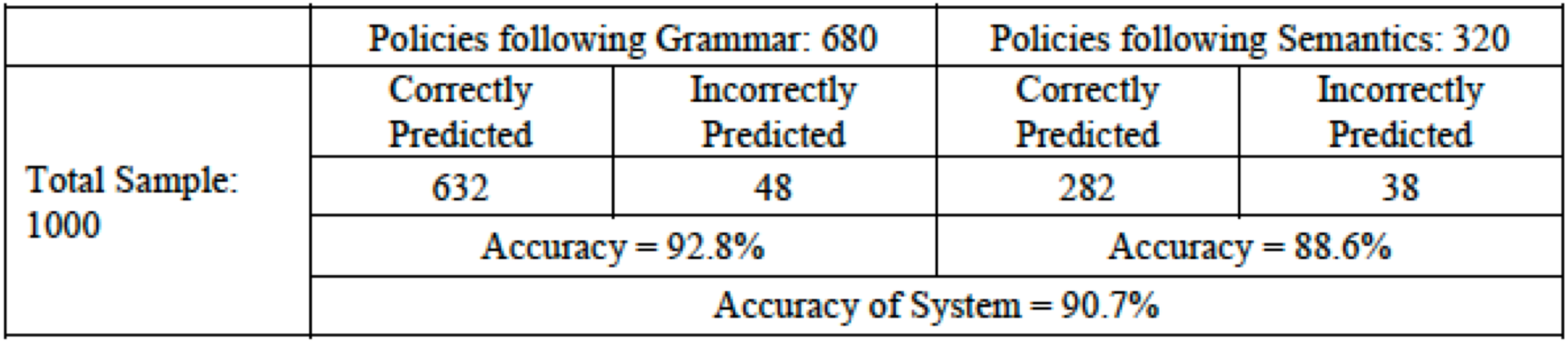




- The combined F1 Score is constant between 0.9 – 0.95 ending at 0.905 for 1000 inputs
- The number of correctly predicted policies is high, which defines the reliability of the system
- F1 Score varies for inputs from different users, increasing slightly with improved knowledge

Accuracy

- Accuracy: The number of correctly interpreted policies by total number of input policies



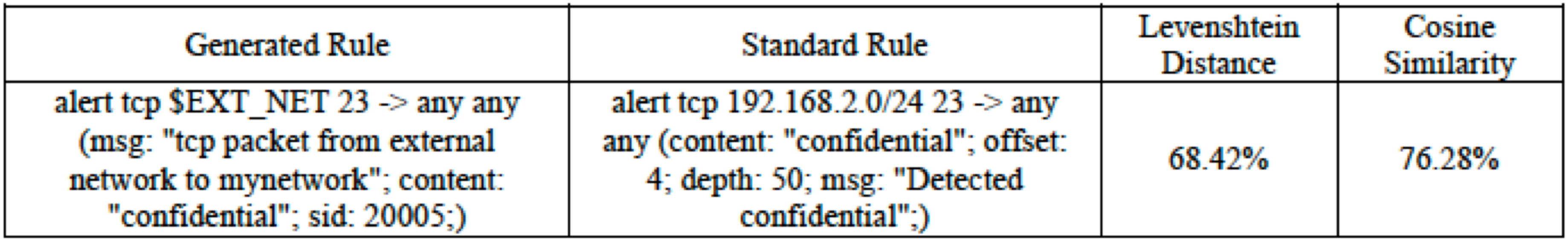
	Policies following Grammar: 680		Policies following Semantics: 320	
Total Sample: 1000	Correctly Predicted	Incorrectly Predicted	Correctly Predicted	Incorrectly Predicted
	632	48	282	38
	Accuracy = 92.8%		Accuracy = 88.6%	
	Accuracy of System = 90.7%			

- Accuracy here is the weighted accuracy calculated from the individual accuracies of grammar and semantics engines
- Accuracy can be improved by making the semantics engine robust in interpreting the input policies.

Similarity Examples

"generate alert when tcp packets from external network to mynetwork with content confidential”

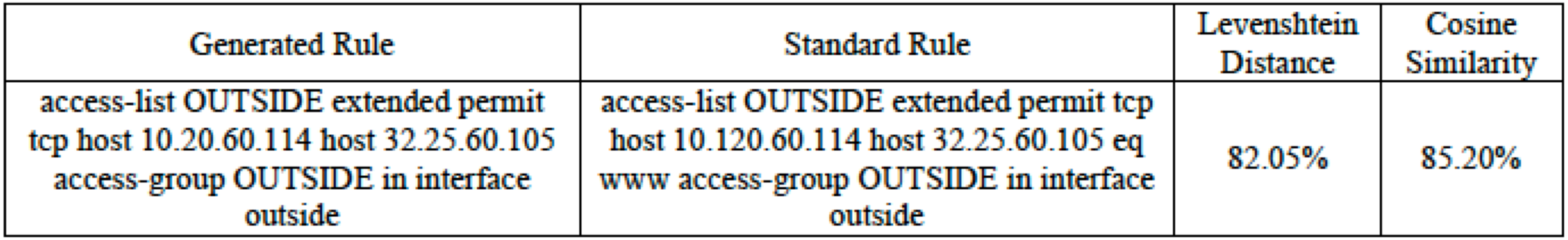
Snort IDS



Generated Rule	Standard Rule	Levenshtein Distance	Cosine Similarity
alert tcp $EXT_NET 23 -> any any (msg: "tcp packet from external network to mynetwork"; content: "confidential"; sid: 20005;)	alert tcp 192.168.2.0/24 23 -> any any (content: "confidential"; offset: 4; depth: 50; msg: "Detected confidential";)	68.42%	76.28%

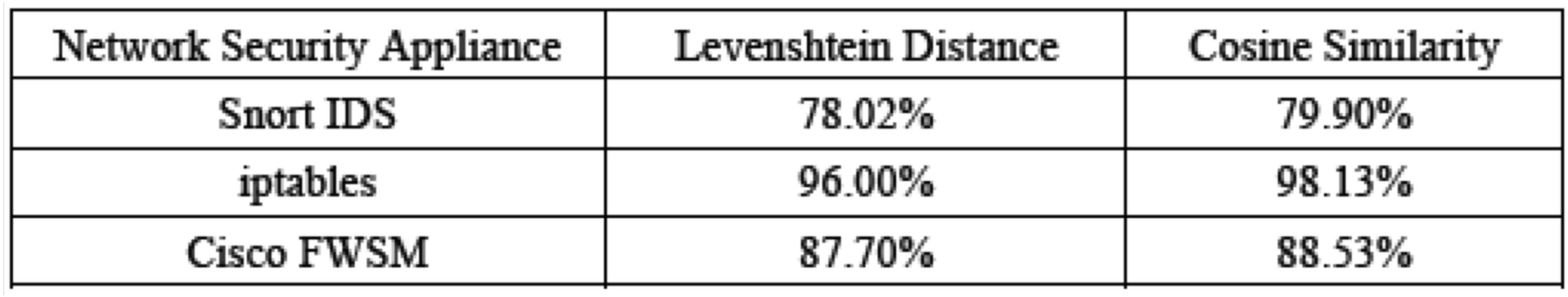
"allow facebook to hostA"

Cisco FWSM

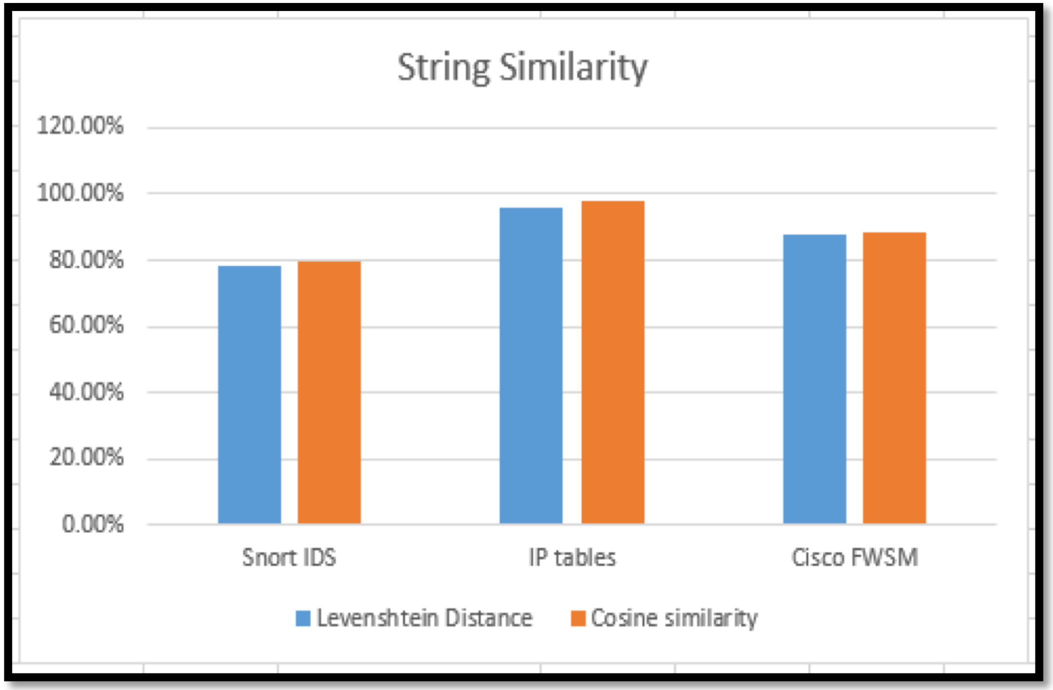


Generated Rule	Standard Rule	Levenshtein Distance	Cosine Similarity
access-list OUTSIDE extended permit tcp host 10.20.60.114 host 32.25.60.105 access-group OUTSIDE in interface outside	access-list OUTSIDE extended permit tcp host 10.120.60.114 host 32.25.60.105 eq www access-group OUTSIDE in interface outside	82.05%	85.20%

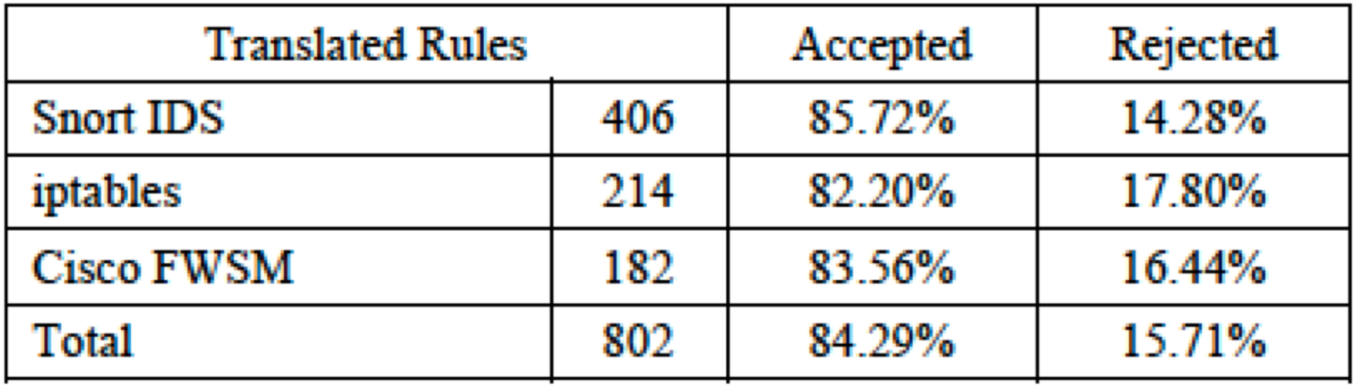
Similarity with Standard Rule



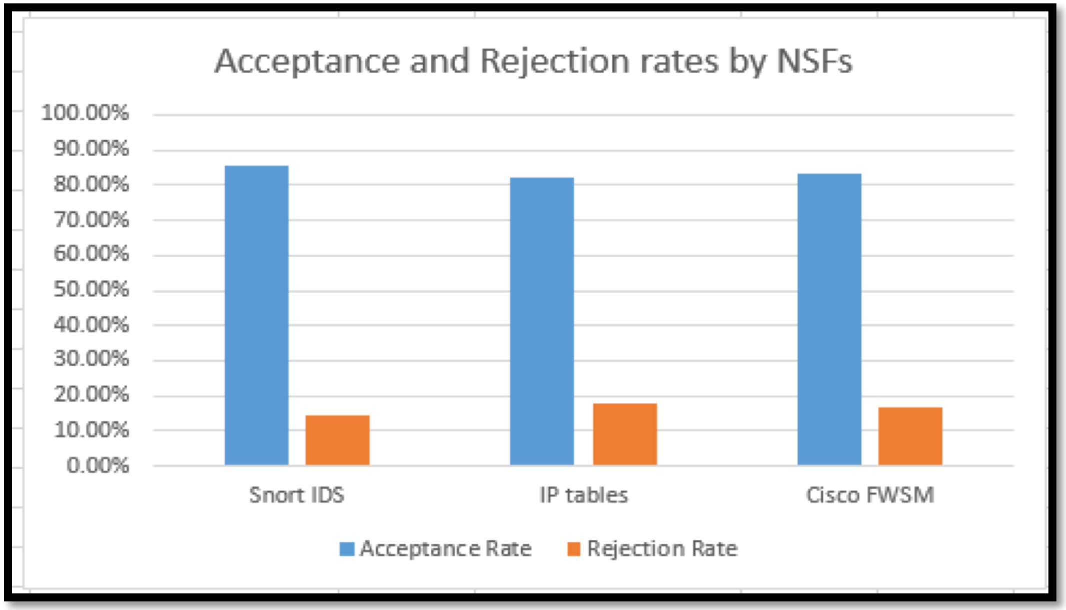
Network Security Appliance	Levenshtein Distance	Cosine Similarity
Snort IDS	78.02%	79.90%
iptables	96.00%	98.13%
Cisco FWSM	87.70%	88.53%



Acceptance and Rejection Rates



Translated Rules		Accepted	Rejected
Snort IDS	406	85.72%	14.28%
iptables	214	82.20%	17.80%
Cisco FWSM	182	83.56%	16.44%
Total	802	84.29%	15.71%



Reasons for Rejection

- Redundant Base
- Redundant Overlapping
- Duplicate
- Conflicting

Conclusion

- Cybersecurity is becoming a more pervasive and complex problem, resulting in an urgent need to establish flexible, collaborative security mechanisms for our common defense
  - This research work is about developing a reliable system using human language inputs and accurately translate them into machine understandable security rules
  - Security is everyone's shared responsibility
- Some key points
  - Started in the 1970s, Neighborhood Watch programs established stronger communities and built trust that brought members together to deter would-be criminals
  - The Internet provides an unbounded value proposition for massive collaboration

Conclusion (cont’d)

- Based on our mostly positive results, there is a lot of promise for community engagement
  - Technologically average individuals can engage meaningfully and effectively with network security appliances
  - Network security appliances are able to translate natural language correctly and effectively
- But it is pretty clear that we need both education and feedback for users and on network security appliances
  - There are still limits with user education, training, and awareness
  - Text box field for experts, pull-down menus for non-experts
- NLP can improve accuracy, even with diverse input
- But there is still a lot of work to do!

Future Work

- Implement standard NLP techniques such as a part-of-speech tagger (POS Tagger) to improve accuracy
  - Improve NLP techniques for semantics and syntax
- Integrate voice recognition for audio input
- Increased analysis of network security appliance logs at interfaces
  - Construction of precise security rules with options
- Extend tool capability using machine learning techniques
- Add support for large number of diverse network security appliances