

# The Statue of Liberty

## Combining Default Deny IPS and Active HoneyPots

"Give me your tired, your poor, your  
huddled masses yearning to breathe  
free...once you have passed through  
security on Ellis Island, of course."

By Philip Trainor

[ptrainor@imperfectnetworks.com](mailto:ptrainor@imperfectnetworks.com)

Black Hat Briefings USA 2006



# Change the way you think about IPS

- All networks need a plan for a breach in security
- Intrusion Prevention Systems with large pattern matching rule sets are never going to provide complete security



# ■ This presentation will entail:

- 1. How to create a default deny IPS
- 2. How to create an active honey pot
- 3. The Statue of Liberty uses these concepts together for an improved security model



# The Majority of Network Security Problems:

1. People who create and use networks
2. The networks

People's issues are too difficult to address so we will focus on the networks.

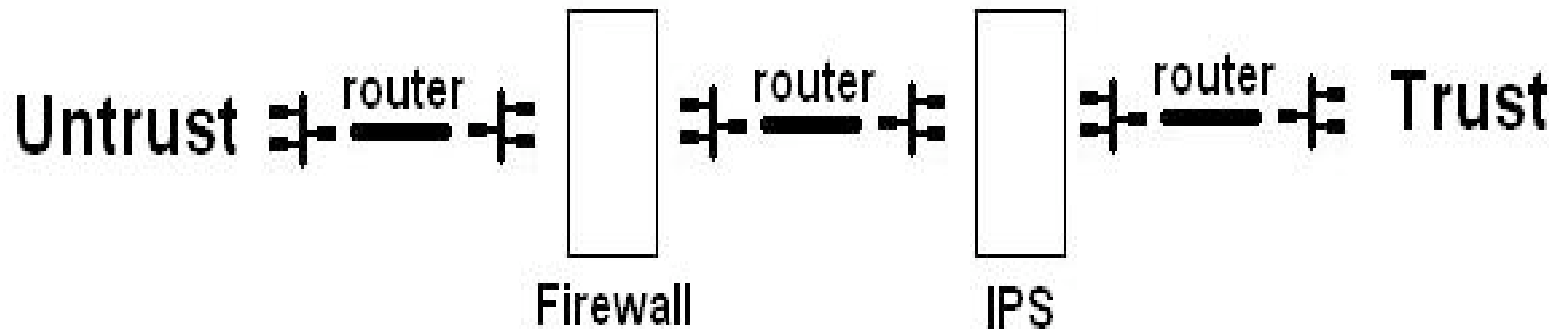


## Two major problems concerning security with information sharing networks:

- It is impossible to deliver a completely secure network solution.
- Most network security models have no plan for an inevitable breach in security.



A layered security model:  
Trusted services are protected  
by an inline firewall and  
intrusion prevention system.



# The Purpose of Firewalls: Default Deny

Block in all  
Block out all

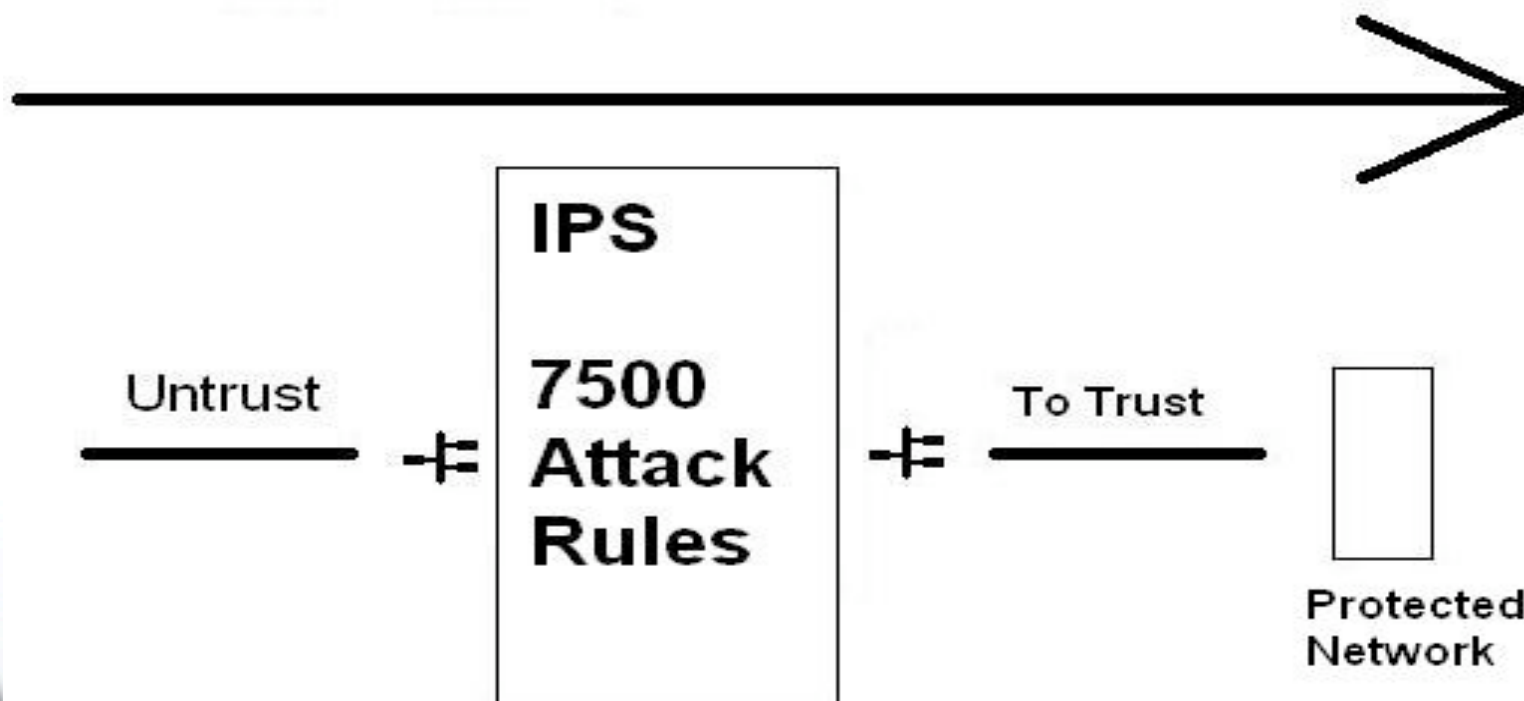
This should be at the default setting for every firewall rule set.

After these rules should come carefully crafted 'pass' rules to allow access within the scope of a network's purpose



# Many Intrusion Prevention Systems are default PASS

- If traffic does not match a blocking rule...





# More Issues...

- Difficult to create signatures for custom applications on public networks(ASP.NET, soap, cgi, etc)
- Most commercial software is still not being created with sufficient concern towards future security implications



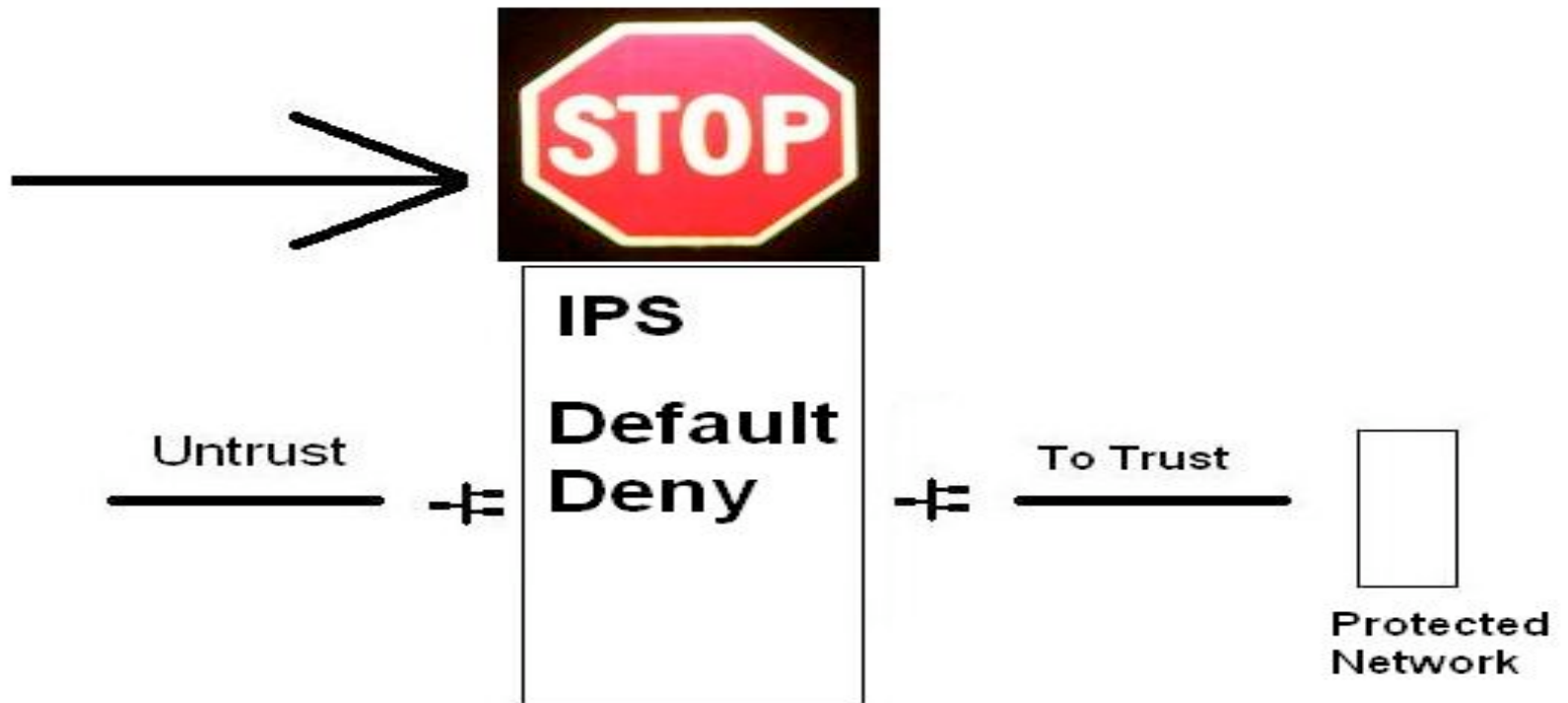
# Vulnerable to attacks when...

1. A new exploit has been created
2. Proof of concept code has been posted
3. No IPS policy has been created



# A solution: Default Deny IPS

A new attack never reaches protected services.  
Traffic is sent to Active Honey Pot for analysis.



# What is good traffic?

- Has never caused an issue:
  - GET / HTTP/1.0
  - RFC Formatted DNS Query response
  - SMTP HELO Server
  - (known good strings from /etc/httpd/logs)
- A new problem:
  - How to build the ruleset
  - False positives

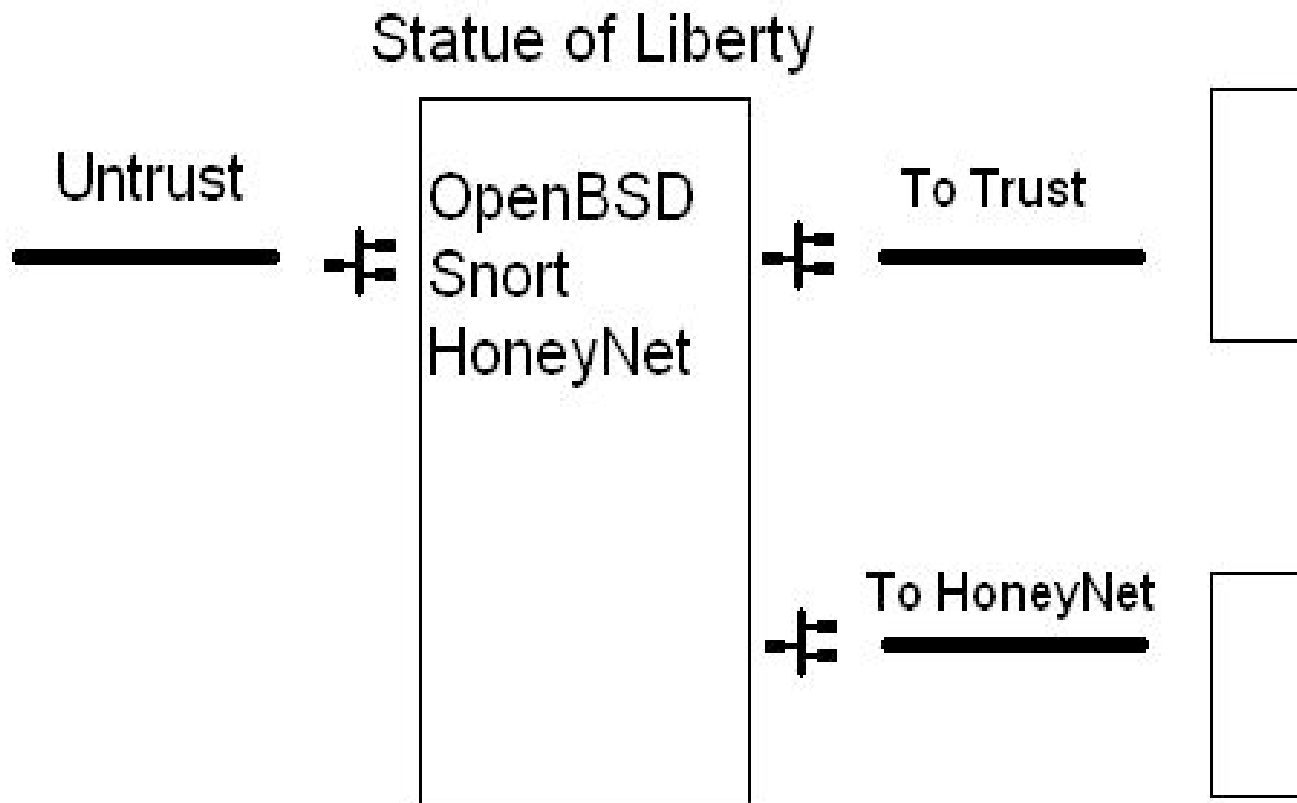


# The Statue of Liberty is ONE solution

- The security community (represented here) should expand the idea
- Code for the Statue of Liberty will be posted online



# Architectural Design of the Statue



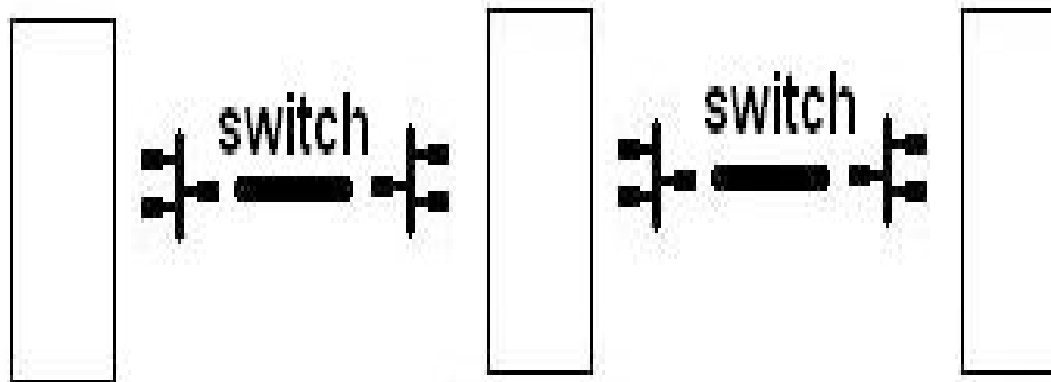
# The Guts

- OpenBSD with 2 NIC's using pf ruleset to route traffic to Active HoneyPot or Protected Network
  - SYN proxy
  - Scrub
  - defragment
- Inline Snort modified to only route traffic to real service iff matches rule
- If there is no rule match goes to HoneyNet Gateway



# Active Honey Pots

- Virtual machines are suspended after a potential attacks to save environment for analysis
- After an attack a new VM is spawned



Statue of Liberty

Honey Net Gateway

R00 / Virtual Machine





# HoneyNet Project uses

- Data Control
- Data Capture
- Data Analysis
- Data Collection



# What are we looking for in traffic?

- Damage to the VM Machine
  - Issues with the host os
  - Issues with the network applications
  - Issues with custom scripts
    - Privilege escalation
    - Crashing
    - Increased resources
    - Creation of new network traffic out of the scope of the application
      - HoneyNet project should never create its own traffic especially traffic attempting to create socket connections or communicate with an outside server



# Live Demonstration of Default Deny IPS using Active HoneyPots

- Scenario 1: Traffic in “Good List”
  - Traffic will be sent from 192.168.1.2 through statue of liberty
  - Traffic matches “known good” traffic in rule set
  - Traffic is routed to real network services



# Live Demonstration of Default Deny IPS using Active HoneyPots

- Scenario 2: Traffic NOT in “Good List” and is NOT Malicious

Matching ruled traffic STILL goes to active honey pot

- Traffic will be sent from 192.168.1.2 through statue of liberty
- Traffic is not in rule set of “known good” traffic
- Traffic is routed to HoneyNet Gateway & analyzed
  - No Crashing
  - No Privilege Escalation
  - No information is gleaned
  - Everything seems copesetic after detailed analysis
- After analyzation a new rule is added to “Good List”



# Live Demonstration of Default Deny IPS using Active HoneyPots

- Scenario 3: Traffic NOT in “Good List” and IS Malicious
  - Traffic will be sent from 192.168.1.2 through statue of liberty
  - Traffic is not in rule set of “known good” traffic
  - Traffic is routed to HoneyNet Gateway & analyzed
    - CRASHING!!!!
    - PRIVILEGE ESCALATION!!!!
    - NETWORK MISUSE!!!
  - After analyzation a new threat is discovered for network services



# What to do with a new threat targeting a commercial vendor?

- My suggestion: Privately inform the proper individuals within said software company.



# Potential flaws, security concerns, and complications with the Statue

- Attacking the system
- New passing rules must be maintained
- Key sharing
- Session oriented traffic takes a turn for the bad.



# Resource Exhaustion...

- 1000's of instances of a new 'Attempt' of an attack
- Statue of liberty should only send one instance of a new attack
- Fuzzing the SOL could be a resource exhaustive technique





# Solution: Don't Throw away default pass IPS

- LAYERED SECURITY WORKS!
- Deploy a tuned, large rule set IPS in front of the statue of liberty
- A default pass IPS with a large rule set will stop 99% of malicious attacks from script kiddies running proof of concept code
- Ideally only ONE instance of an attack will enter the active honeypot.
- Utilizing these services will maximize productivity when analyzing Active Honeypots



# Conclusion

- A default deny IPS combined with Active HoneyPots is a more secure model
- The statue of liberty is an example of a default deny IPS
- The security community should take this example and come up with improvements



# Acknowledgments

- Companies / Projects
  - OpenBSD [www.openbsd.org](http://www.openbsd.org)
  - Snort [www.snort.org](http://www.snort.org)
  - Honey Net [www.honeynet.org](http://www.honeynet.org)
- Individuals
  - Charles McAuley [chuck@lemure.net](mailto:chuck@lemure.net)
  - Seth Hardy [shardy@aculei.net](mailto:shardy@aculei.net)



Thank You!

Q & A

