Network Security Architecture

CS461/ECE422

Computer Security I

Fall 2010

Reading Material

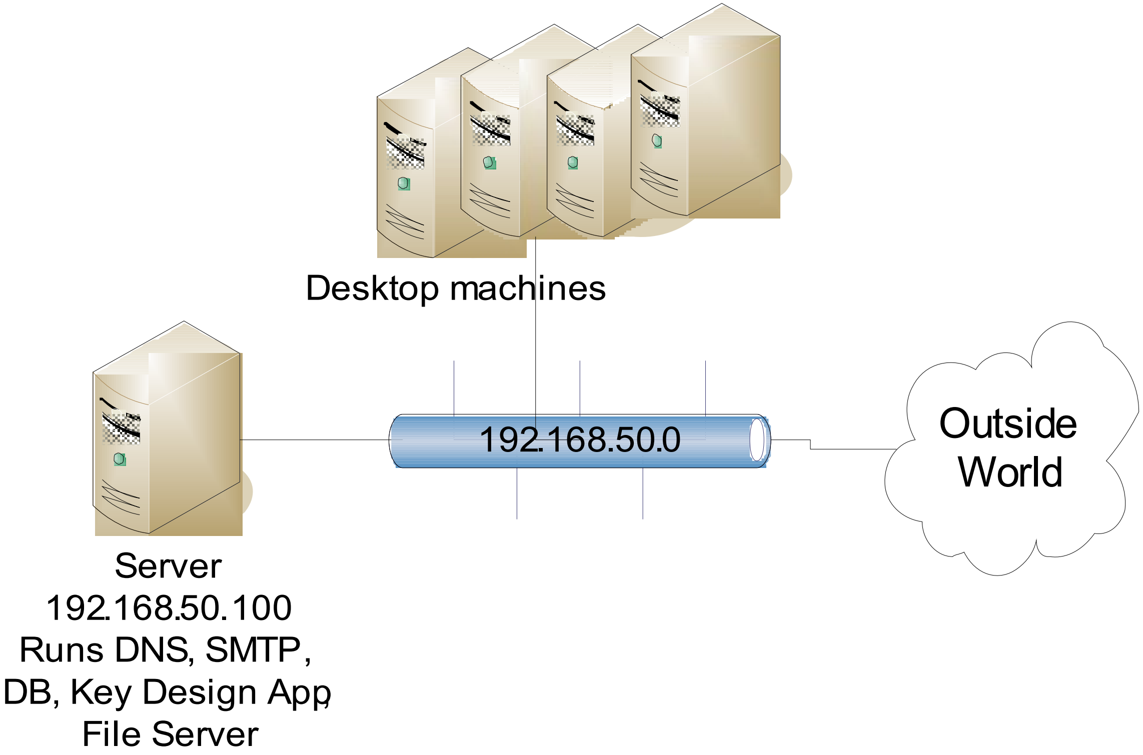
- Computer Security chapter 26.
- “Firewalls and Internet Security: Repelling the Wily Hacker”, Cheswick, Bellovin, and Rubin.
  - New second edition

Overview

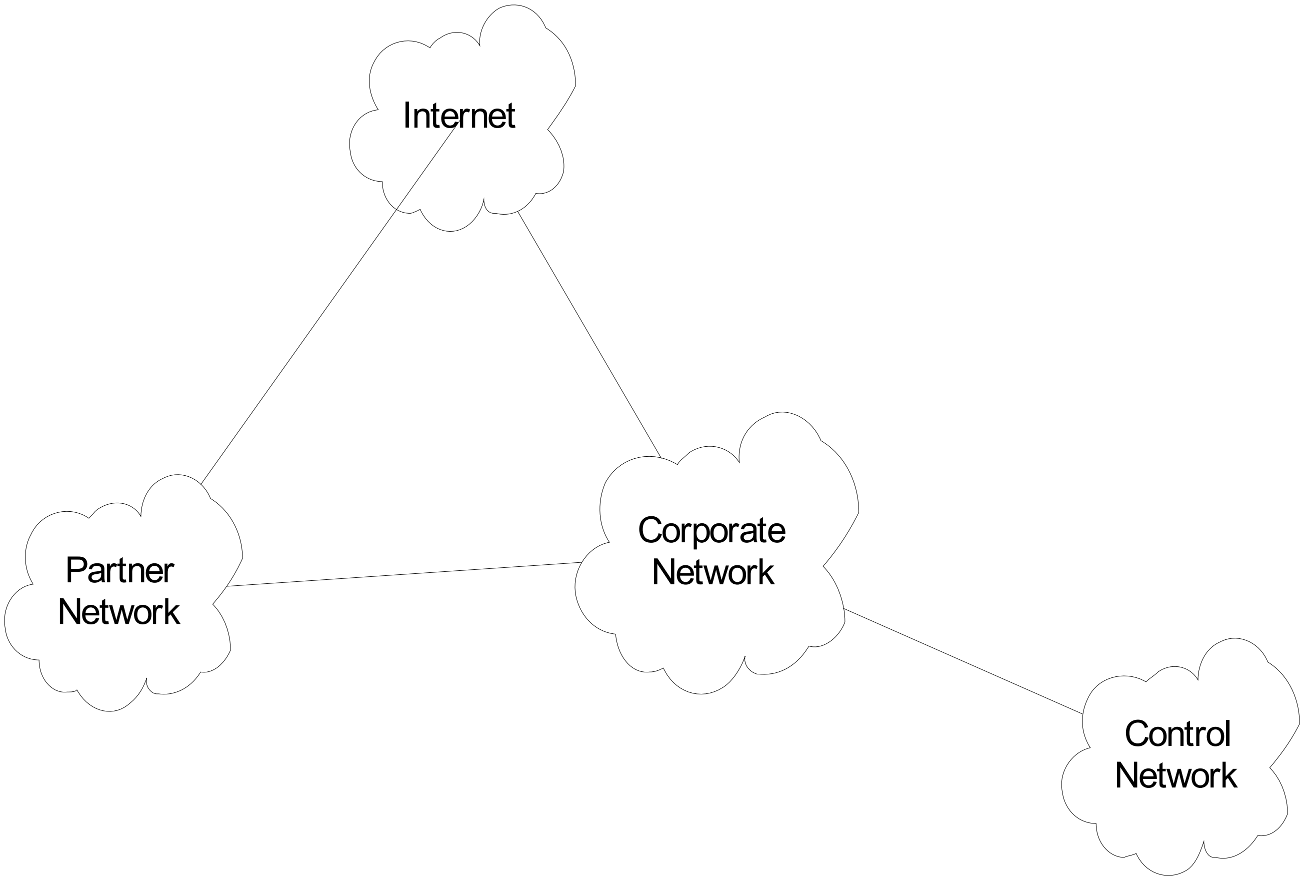
- Network Security Architecture
  - Segmentation
  - Security Domains
  - VPN
- Firewall Technology
  - Address Translation
  - Denial of Service attacks
- Intrusion Detection
- Both firewalls and IDS are introductions.
  - Both are covered in more detail in the Security Lab class.
  - IDS is covered in more detail in 463 – Computer Security.

Segment

- Separate Functionality
  - Limit infection vectors



Security Domains



Virtual Private Networks

- A private network that is configured within a public network
- A VPN “appears” to be dedicated network to customer
- The customer is actually “sharing” trunks and other physical infrastructure with other customers
- Security?
  - Depends on implementing protocol

Multiple VPN Technologies

SSL

- Confidentiality? Yes
- Data integrity? Yes
- User authentication? Yes
- Network access control? No
- In addition, limited traffic

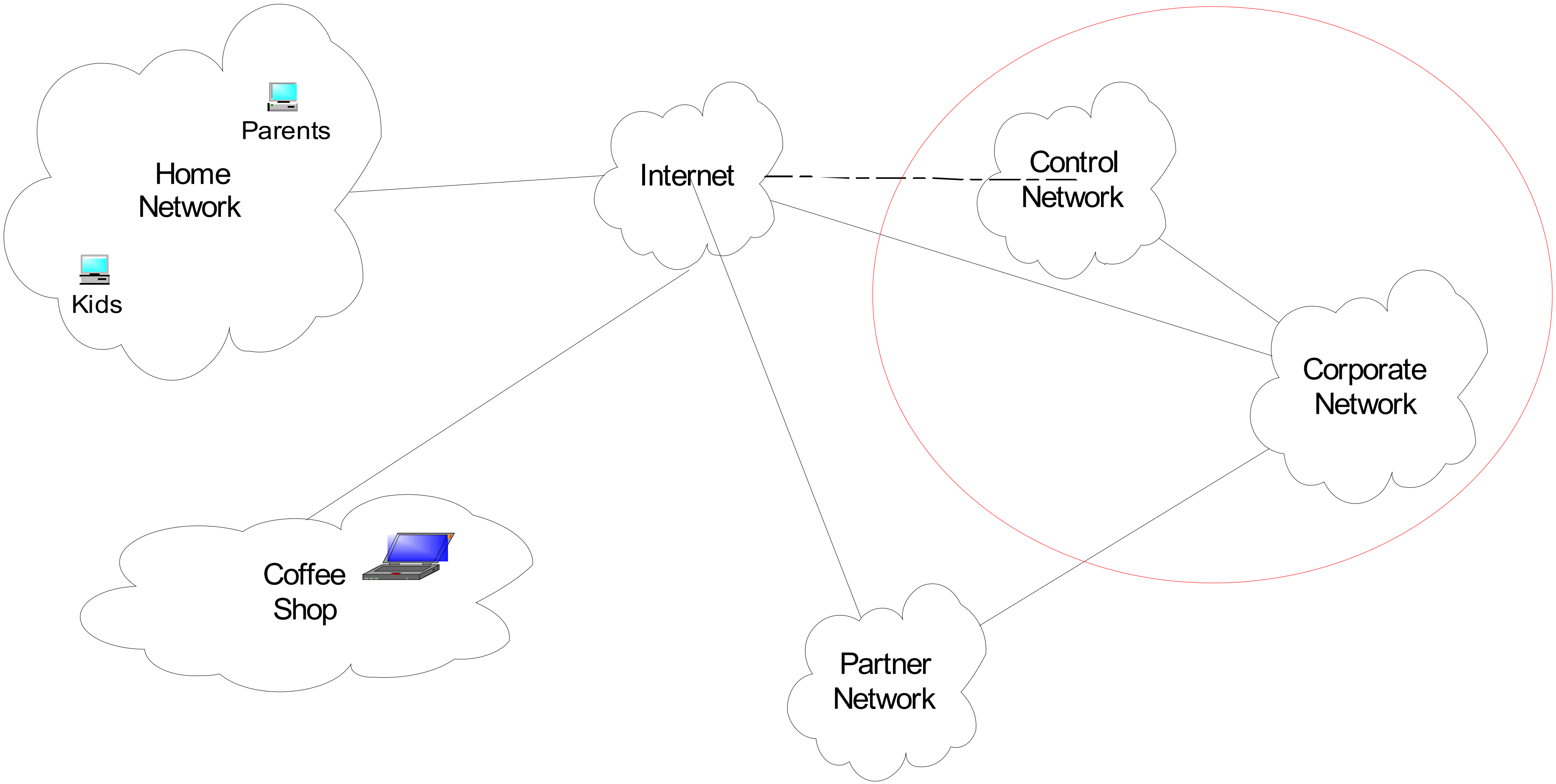
IPSec

- Confidentiality? Yes
- Data Integrity? Yes
- User Authentication? Yes
- Network access control? Yes
- Client configuration required.

VLAN – Layer 2 tunnelling technology

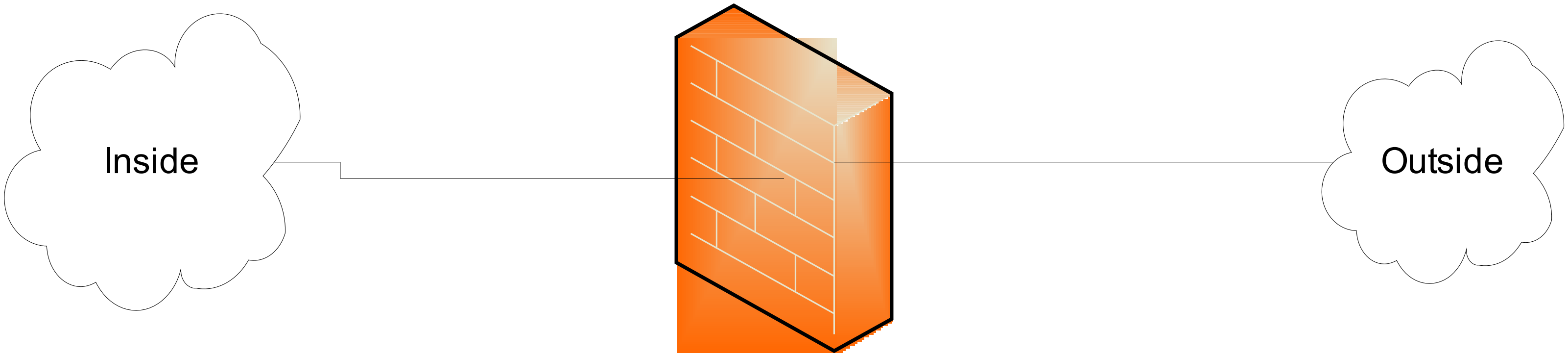
- Confidentiality? No
- Data Integrity? No
- User authentication? Yes
- Network access control? Yes
- Not viable over non-VLAN internetworks

Security Domains with VPNs

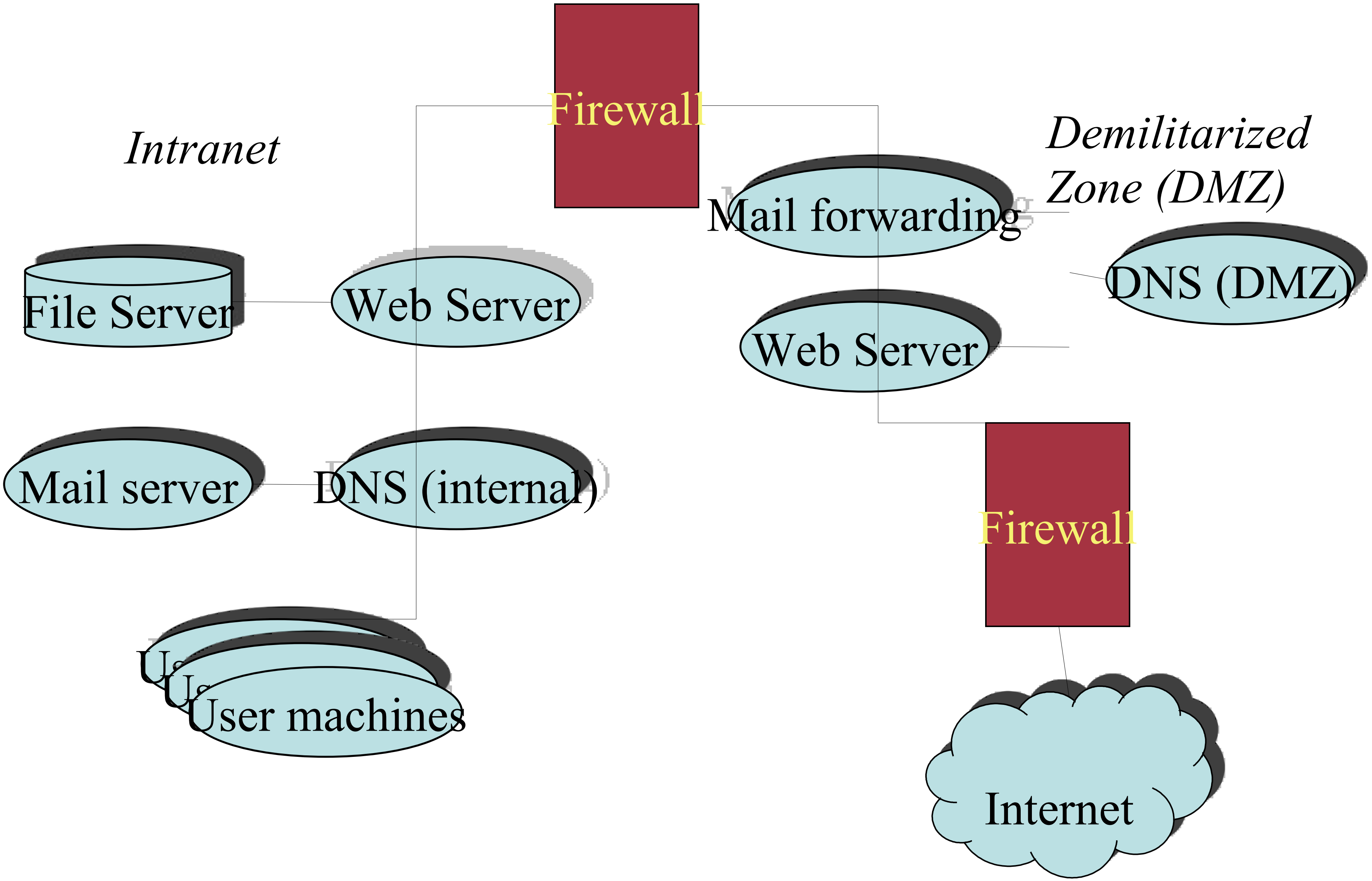


Firewall Goal

- Insert *after the fact security* by wrapping or interposing a filter on network traffic



“Typical” corporate network



Firewall

Intranet

Demilitarized Zone (DMZ)

Mail forwarding

DNS (DMZ)

File Server

Web Server

Web Server

Mail server

DNS (internal)

Firewall

User machines

Internet

Application Proxy Firewall

- Firewall software runs in application space on the firewall
- The traffic source must be aware of the proxy and add an additional header
- Leverage basic network stack functionality to sanitize application level traffic
  - Block java or active X
  - Filter out “bad” URLs
  - Ensure well formed protocols or block suspect aspects of protocol

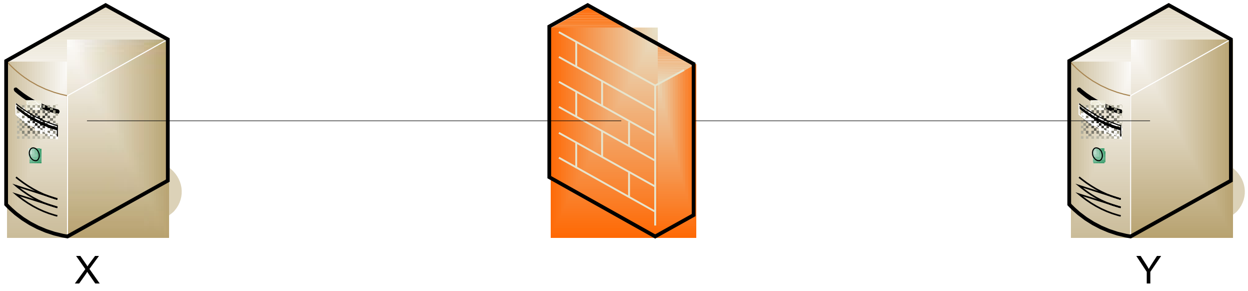
Packet Filter Firewall

- Operates at Layer 3 in router or HW firewall
- Has access to the Layer 3 header and Layer 4 header
- Can block traffic based on source and destination address, ports, and protocol
- Does not reconstruct Layer 4 payload, so cannot do reliable analysis of layer 4 or higher content

Stateful Packet Filters

- Evolved as packet filters aimed for proxy functionality
- In addition to Layer 3 reassembly, it can reconstruct layer 4 traffic
- Some application layer analysis exists, e.g., for HTTP, FTP, H.323
  - Called context-based access control (CBAC) on IOS
  - Configured by fixup command on PIX
- Some of this analysis is necessary to enable address translation and dynamic access for negotiated data channels
- Reconstruction and analysis can be expensive.
  - Must be configured on specified traffic streams
  - At a minimum the user must tell the Firewall what kind of traffic to expect on a port
  - Degree of reconstruction varies per platform, e.g. IOS does not do IP reassembly

Traffic reconstruction



FTP: X to Y
GET /etc/passwd

GET command causes firewall to dynamically open data channel initiate from Y to X

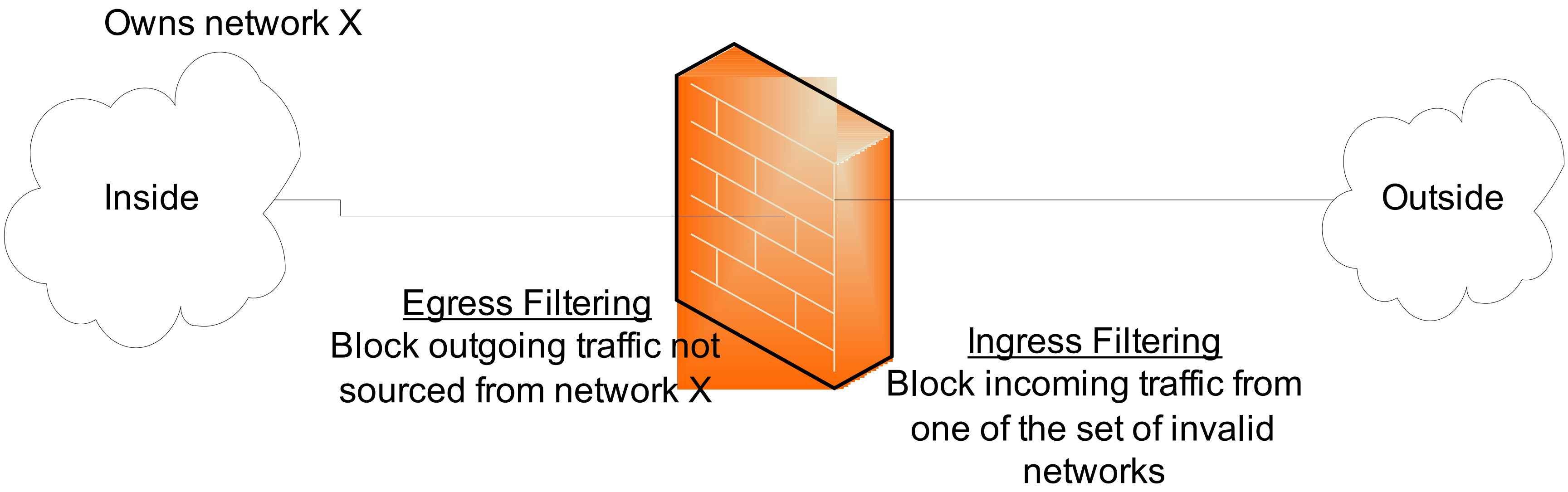
Might have filter for files to block, like /etc/passwd

Access Control Lists (ACLs)

- Used to define traffic streams
  - Bind ACL’s to interface and action
- Access Control Entry (ACE) contains
  - Source address
  - Destination Address
  - Protocol, e.g., IP, TCP, UDP, ICMP, GRE
  - Source Port
  - Destination Port
- ACL runtime lookup
  - Linear
  - N-dimensional tree lookup (PIX Turbo ACL)
  - Object Groups
  - HW classification assists

Ingress and Egress Filtering

- Ingress filtering
  - Filter out packets from invalid addresses before entering your network
- Egress filtering
  - Filter out packets from invalid addresses before leaving your network



Owns network X

Inside

Outside

Egress Filtering
Block outgoing traffic not sourced from network X

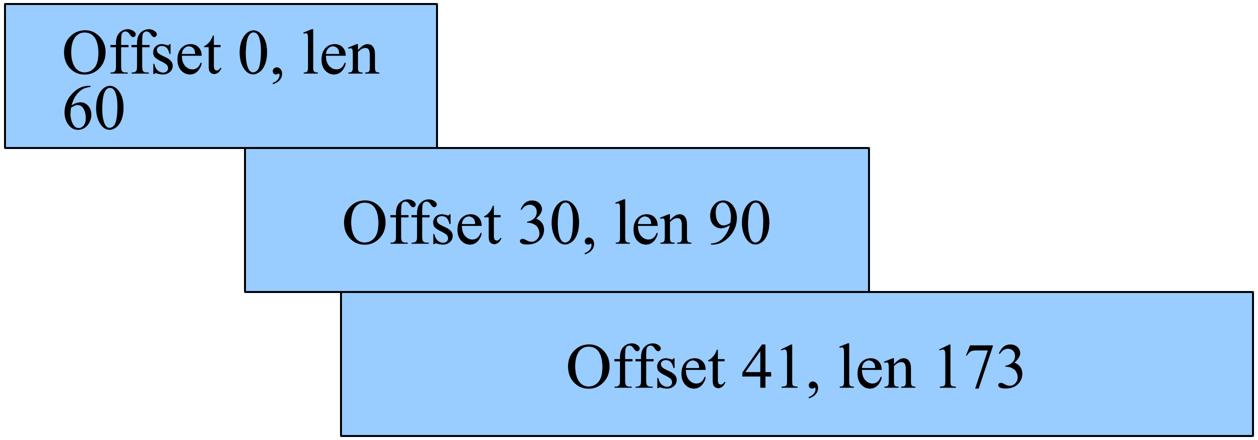
Ingress Filtering
Block incoming traffic from one of the set of invalid networks

Denial of Service

- **Example attacks**
  - **Smurf Attack**
  - **TCP SYN Attack**
  - **Teardrop**
- **DoS general exploits resource limitations**
  - Denial by Consumption
  - Denial by Disruption
  - Denial by Reservation

Teardrop Attack

- Send series of fragments that don't fit together
  - Poor stack implementations would crash
  - Early windows stacks



Offset 0, len 60

Offset 30, len 90

Offset 41, len 173

Address Translation

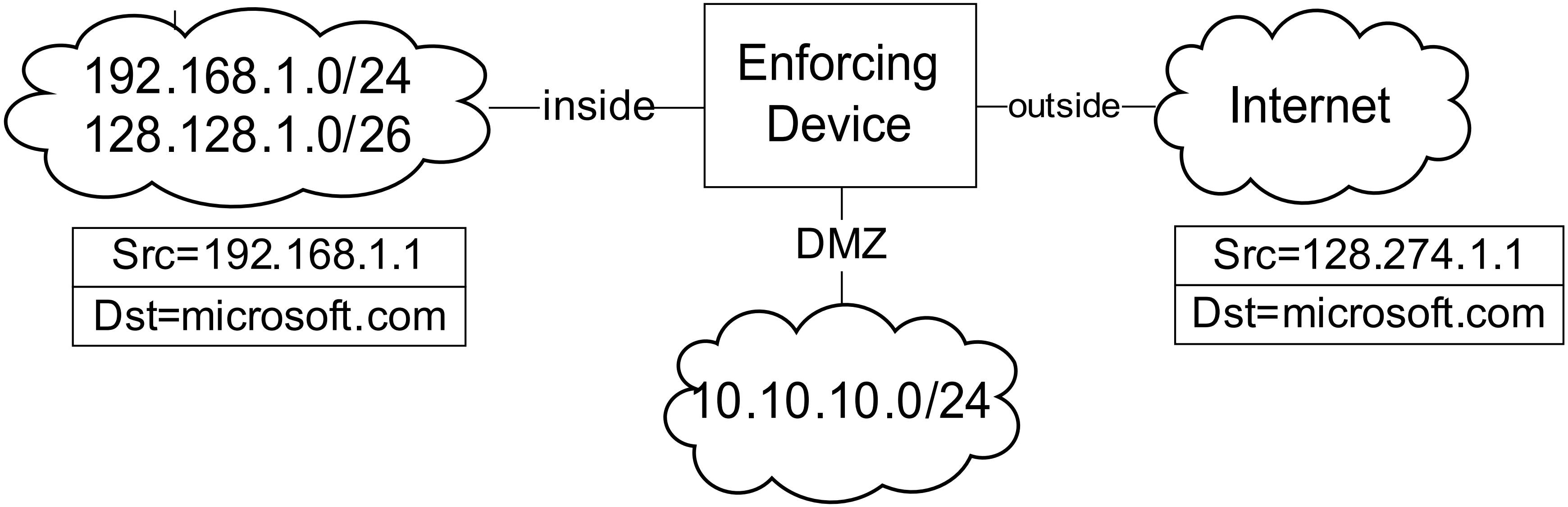
- Traditional NAT RFC 3022 Reference RFC
- Map real address to alias address
  - Real address associated with physical device, generally an unroutable address
  - Alias address generally a routeable associated with the translation device
- Originally motivated by limited access to publicly routable IP addresses
  - Folks didn’t want to pay for addresses and/or hassle with getting official addresses
- Later folks said this also added security
  - By hiding structure of internal network
  - Obscuring access to internal machines
- Adds complexity to firewall technology
  - Must dig around in data stream to rewrite references to IP addresses and ports
  - Limits how quickly new protocols can be firewalled

Address Hiding (NAPT)

- Many to few dynamic mapping
  - Packets from a large pool of private addresses are mapped to a small pool of public addresses at runtime
- Port remapping makes this sharing more scalable
  - Two real addresses can be rewritten to the same alias address
  - Rewrite the source port to differentiate the streams
- Traffic must be initiated from the real side

NAT example

Hide from inside to outside
192.168.1.0/24 behind 128.274.1.1
Static map from inside to DMZ
192.168.1.5 to 128.274.1.5



Src=192.168.1.1
Dst=microsoft.com

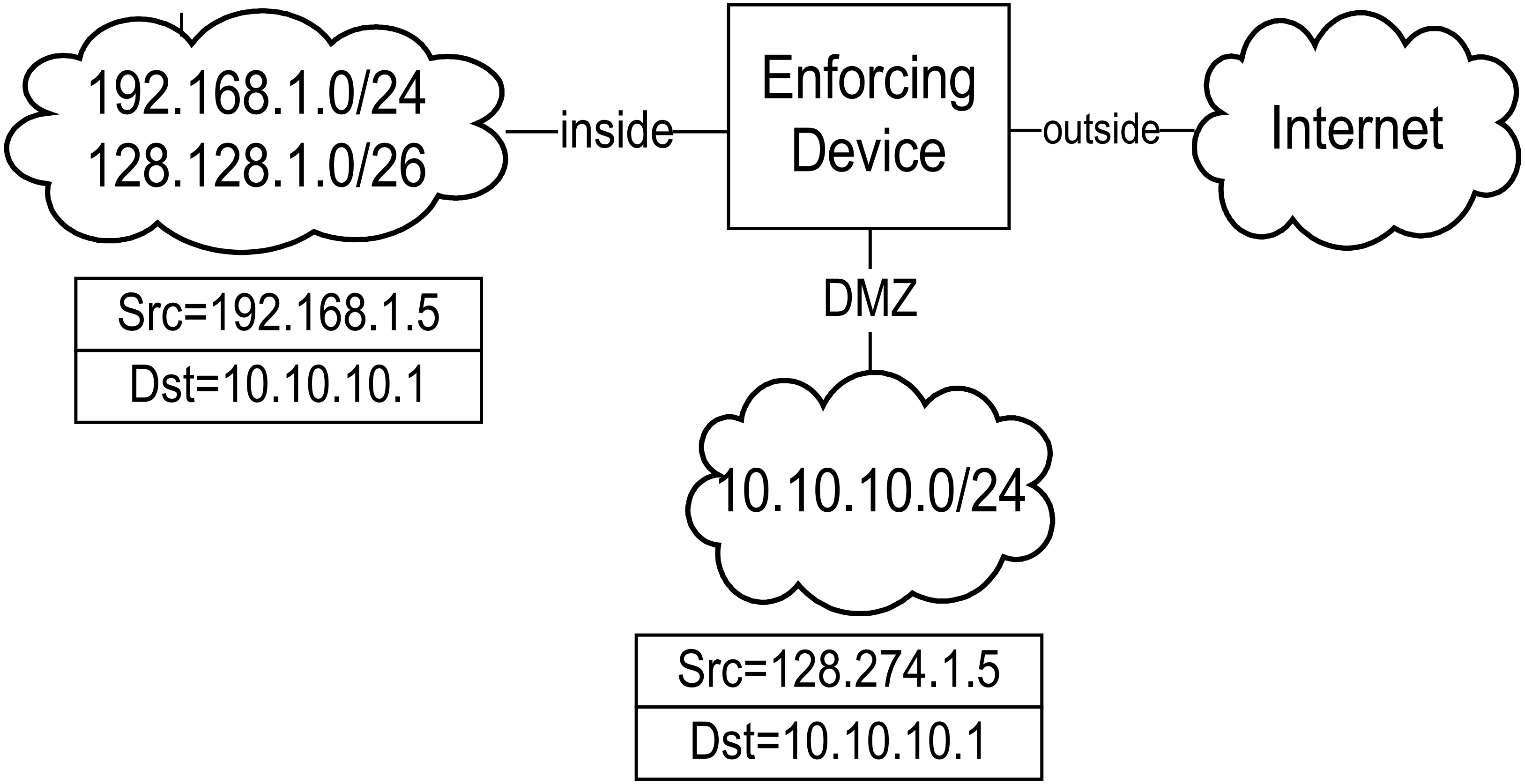
Src=128.274.1.1
Dst=microsoft.com

Static Mapping

- One-to-one fixed mapping
  - One real address is mapped to one alias address at configuration time
  - Traffic can be initiated from either side
- Used to statically map out small set of servers from a network that is otherwise hidden
- Static port remapping is also available

NAT example

Hide from inside to outside
192.168.1.0/24 behind 128.274.1.1
Static map from inside to DMZ
192.168.1.5 to 128.274.1.5



Intrusion Detection

- Holy Grail: Detect and correct “bad” system behaviour
- Detection can be viewed in two parts
  - Anomaly detection: Use statistical techniques to determine unusual behavior
  - Mis-use detection: Use signatures to determine occurrence of known attacks
- Detection can be performed on host data (HIDS), network data (NIDS), or a hybrid of both

IDS Architecture

- Agents run at the lowest level gathering data. Perform some basic processing.
- Agents send data to a Director that performs more significant processing of the data. Potentially there is a hierarchy of agents and directors
  - Director has information from multiple sources and can perform a time-based correlation to derive more significant actions
- Directors invoke Notifiers to perform some action in response to a detected attack
  - Popup a window on a screen
  - Send an email or a page
  - Send a new syslog message elsewhere.
  - Adjust a firewall or some other policy to block future action from the attacker

Data Sources

- Direct data
  - Network packets
  - System calls
- Indirect data
  - Syslog data, Windows event logs
  - Events from other intrusion detection systems
  - Netflow information generated by routers about network traffic

Mis-use/Signature Detection

- Fixed signatures are used in most deployed IDS products
  - E.g., Cisco, ISS, Snort
- Like virus scanners, part of the value of the product is the team of people producing new signatures for newly observed malevolent behavior
- The static signature mechanism has obvious problems in that a dedicated attacker can adjust his behaviour to avoid matching the signature.
- The volume of signatures can result in many false positives
  - Must tune the IDS to match the characteristics of your network
  - E.g., what might be unusual in a network of Unix systems might be normal in a network of Windows Systems (or visa versa)
  - Can result in IDS tuned too low to miss real events
  - Can hide real attacks in the mass of false positives

Example Signature

- Signature for port sweep
  - A set of TCP packets attempting to connect to a sequence of ports on the same device in a fixed amount of time
- In some environments, the admin might run nmap periodically to get an inventory of what is on the network
  - You would not want to activate this signature in that case

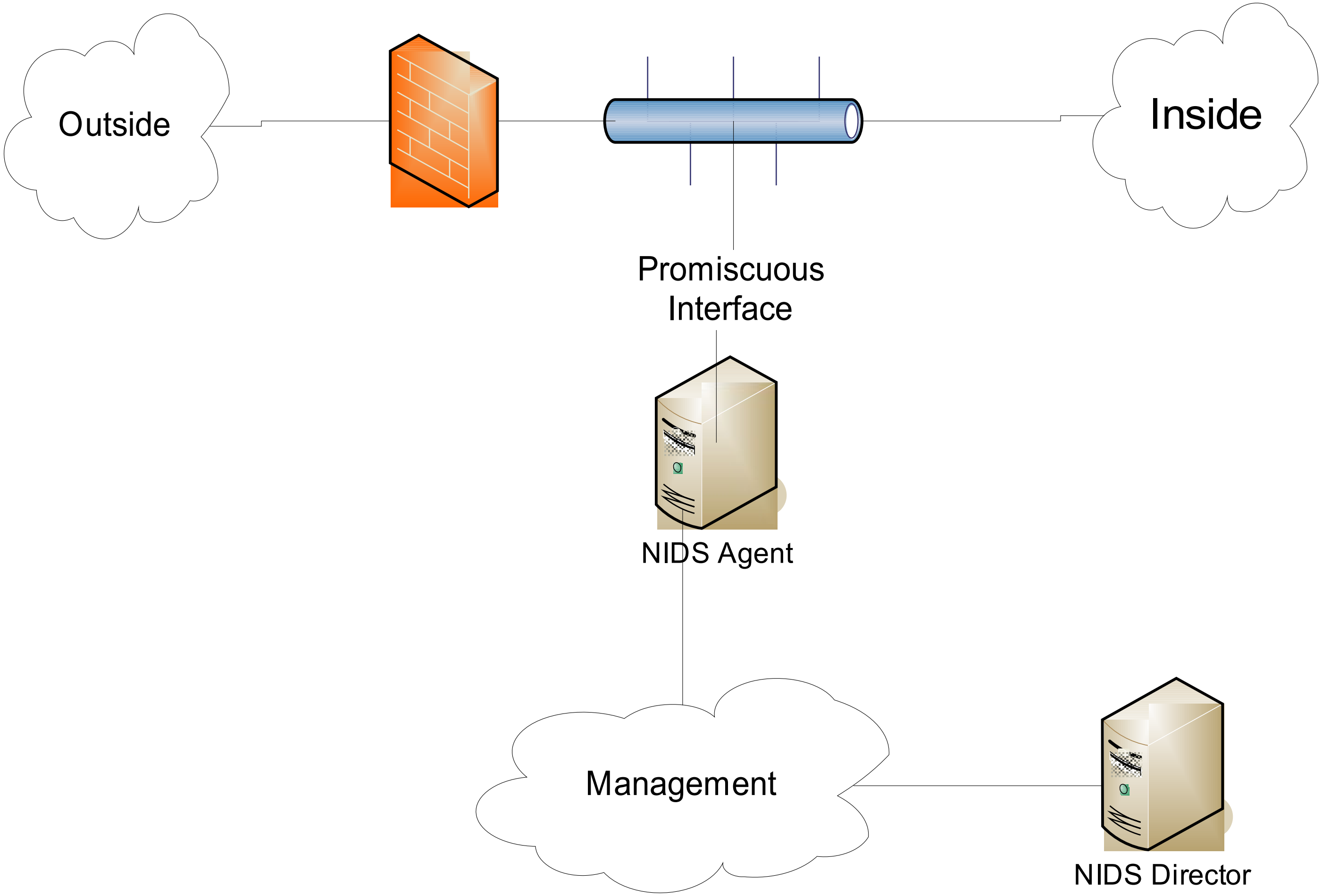
Anomaly/statistical detection

- Seems like using statistics will result in a more adaptable and self-tuning system
  - Statistics, neural networks, data mining, etc.
- How do you characterize normal?
  - Create training data from observing “good” runs
    - E.g., Forrest’s program system call analysis
  - Use visualization to rely on your eyes
- How do you adjust to real changes in behaviour?
  - Gradual changes can be easily addressed. Gradually adjust expected changes over time
  - Rapid changes can occur. E.g., different behaviour after work hours or changing to a work on the next project

Host Based IDS

- Tripwire – Very basic detection of changes to installed binaries
- More recent HIDS. Look at patterns of actions of system calls, file activity, etc. to permit, deny, or query operations
  - Cisco Security Agent
  - Symantec
  - McAfee Entercept

Classical NIDS deployment



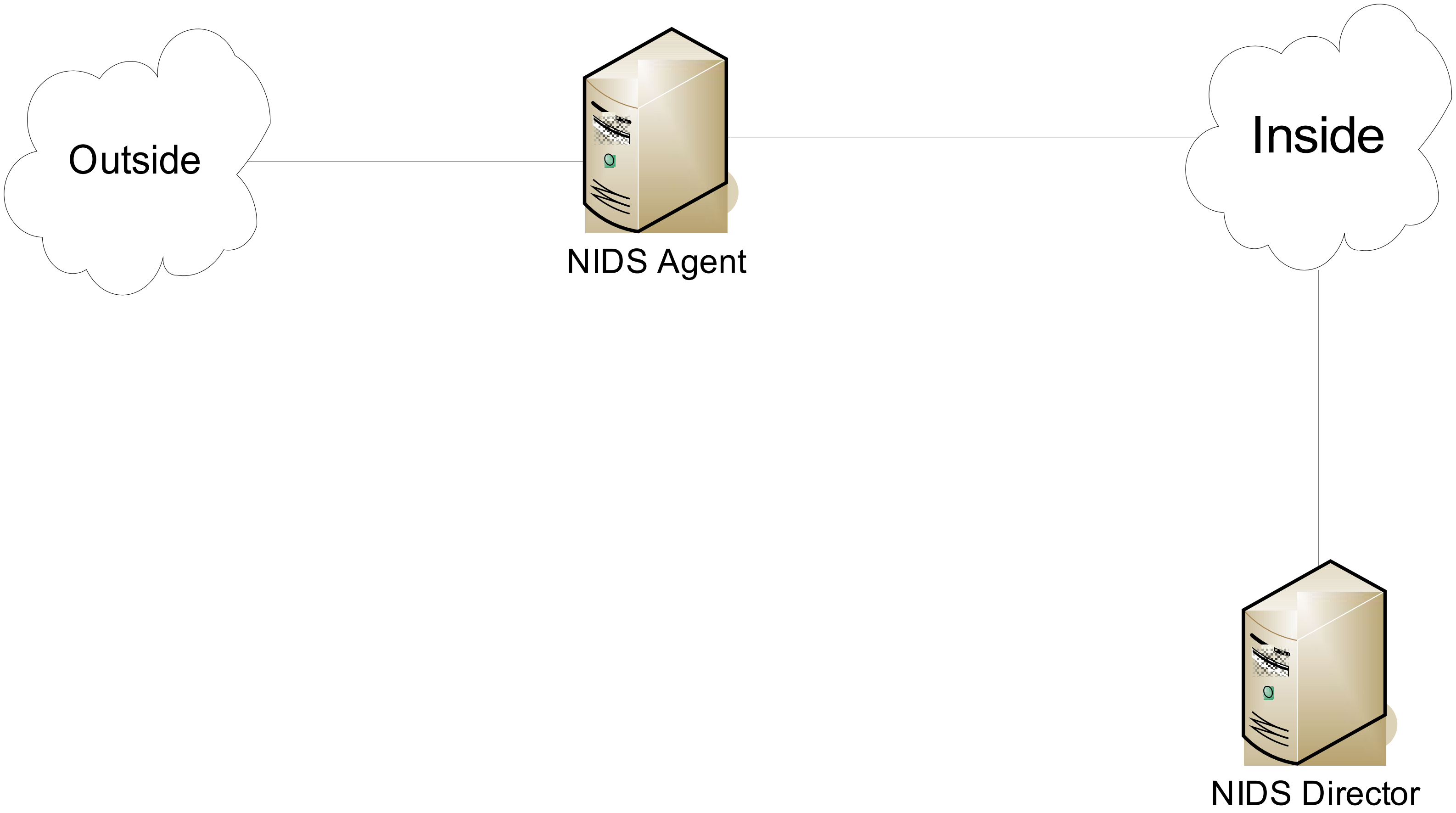
NIDS Remediation Options

- Log the event
- Drop the connection
- Reset the connection
- Change the configuration of a nearby router or firewall to block future connections

Intrusion Protection Systems (IPS)

- Another name for inline NIDS
- Latest buzz among the current NIDS vendors
- Requires very fast signature handling
  - Slow signature handling will not only miss attacks but it will also cause the delay of valid traffic
  - Specialized hardware required for high volume gateways
- When IDS is inline, the intrusion detector can take direct steps to remediate.
- If you move IDS into the network processing path, how is this different from really clever firewalling?

Network IPS scenario



Honey Pots

- Reconnaissance for the good guys
- Deploy a fake system
  - Observe it being attacked
- Resource management
  - Cannot be completely passive
    - Must provide enough information to keep attacker interested
  - Must ensure that bait does not run away
- Scale
  - Host, network, dark address space

Summary

- Identification of security domains basis of perimeter security control
  - Firewall is the main enforcer
- Intrusion detection introduces deeper analysis and potential for more dynamic enforcement
- Intermediate enforcement can handle some Denial of Service attacks