Firewall Technology

Cyber Security

Spring 2010

Outline

- Basics of firewalling
  - Architectures
  - Network Address Translation
  - Logging
- Advanced Topics
  - Identity in firewalls
  - Multiple security levels
- Firewall Futures

Reading Material

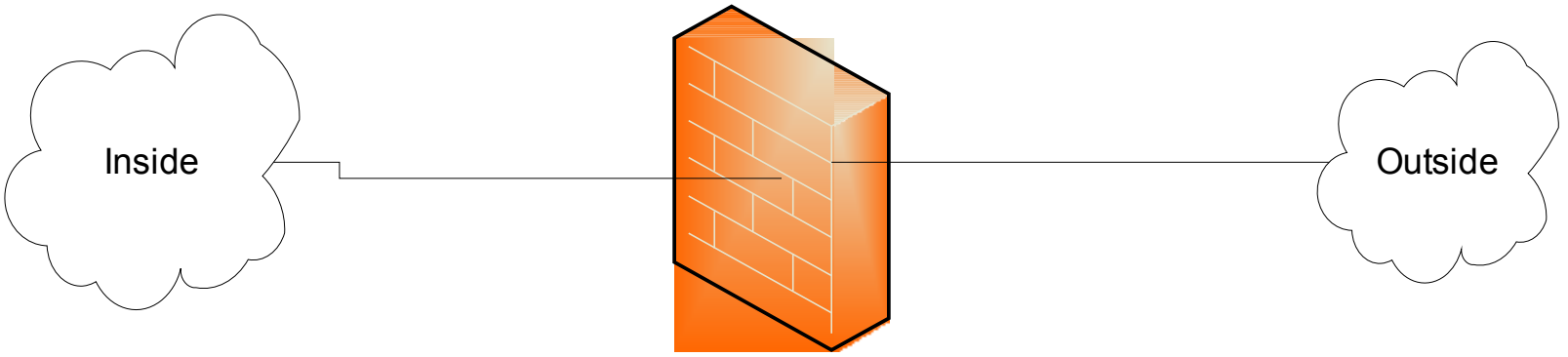
- “Firewalls and Internet Security: Repelling the Wily Hacker”, Cheswick, Bellovin, and Rubin.
  - New second edition
- “Network Security Principles and Practices”, Sadaat Malik
  - Cisco oriented
- PIX 7.0 Configuration Guide http://www.cisco.com/en/US/products/ps6120/products_configuration_guide_book09186a0080450278.html
- PIX 7.0 Command Reference http://www.cisco.com/en/US/products/ps6120/products_command_reference_book09186a00805fbad6.html
- “Firewall and Internet Security, the Second Hundred (Internet) Years” http://www.cisco.com/warp/public/759/ipj_2-2/ipj_2-2_fis1.html
  - A firewall overview article from 1999

Presentation Bias

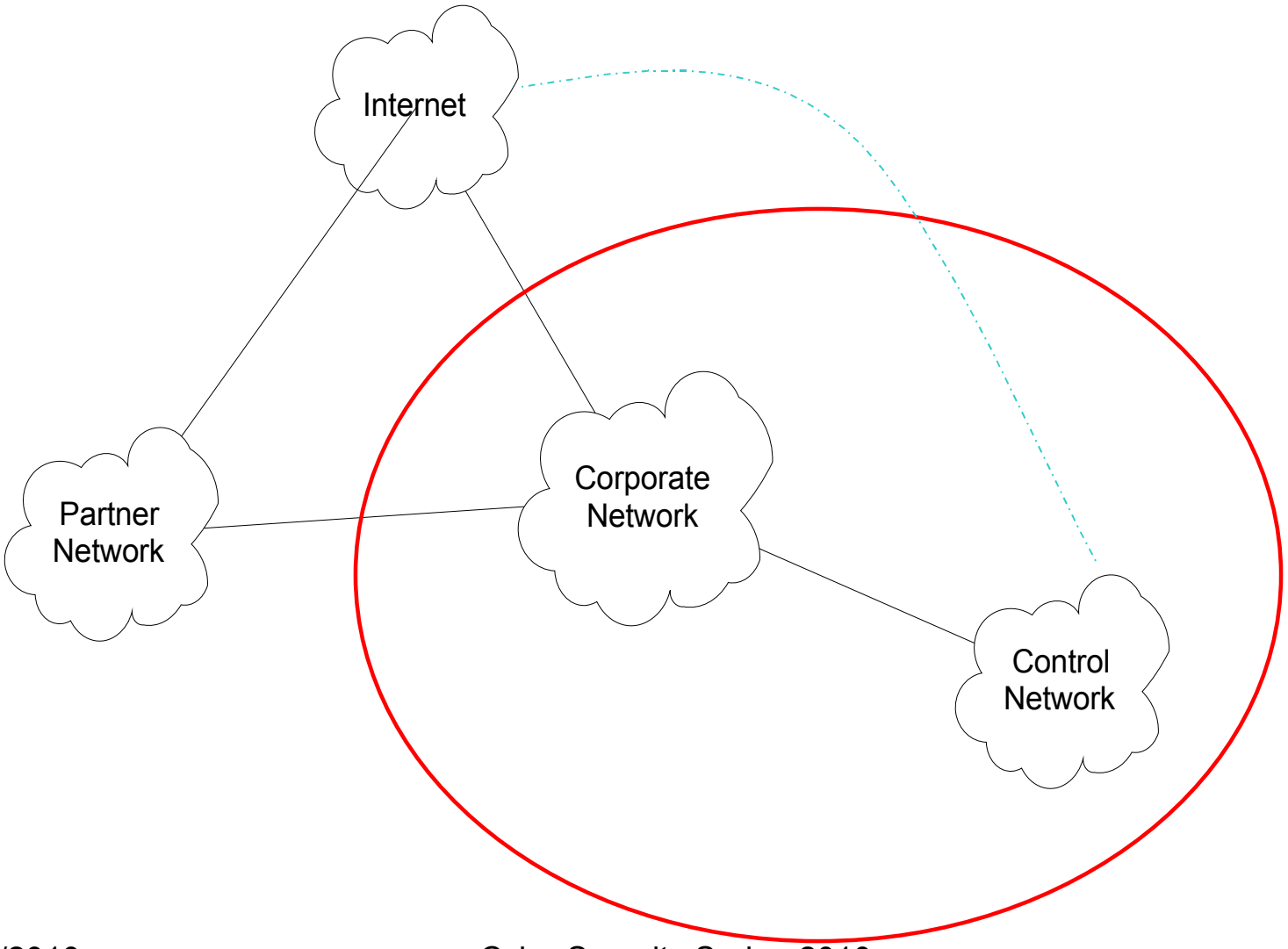
- Talking from my experience
  - Colored by Cisco Firewalls: Centri, PIX, IOS FW, Firewall Service Module
  - More recently iptables
- The enterprise firewall producers chase each other so similar issues arise in Netscreen (Juniper) and Checkpoint
- Personal firewalls address a subset of the issues that Enterprise Firewalls do

Firewall Goal

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



Security Domains



Several Firewall Styles

- Differ primarily on what layers of the network stack they consider
  - Packet Filter
  - Application Proxy
  - Stateful Packet Filter

Application Proxy

- 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
- Not used much anymore

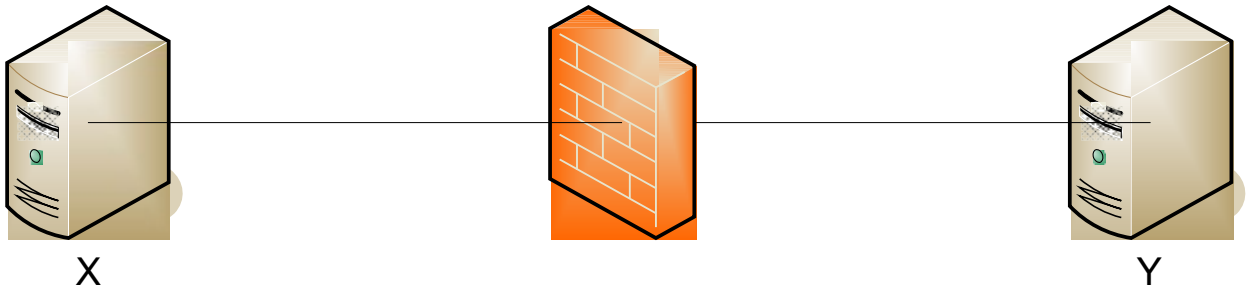
Packet Filter

- 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, e.g., port 80 is just a clue that the incoming traffic will be HTTP
  - Degree of reconstruction varies per platform, e.g. IOS does not do IP reassembly

Traffic reconstruction



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)

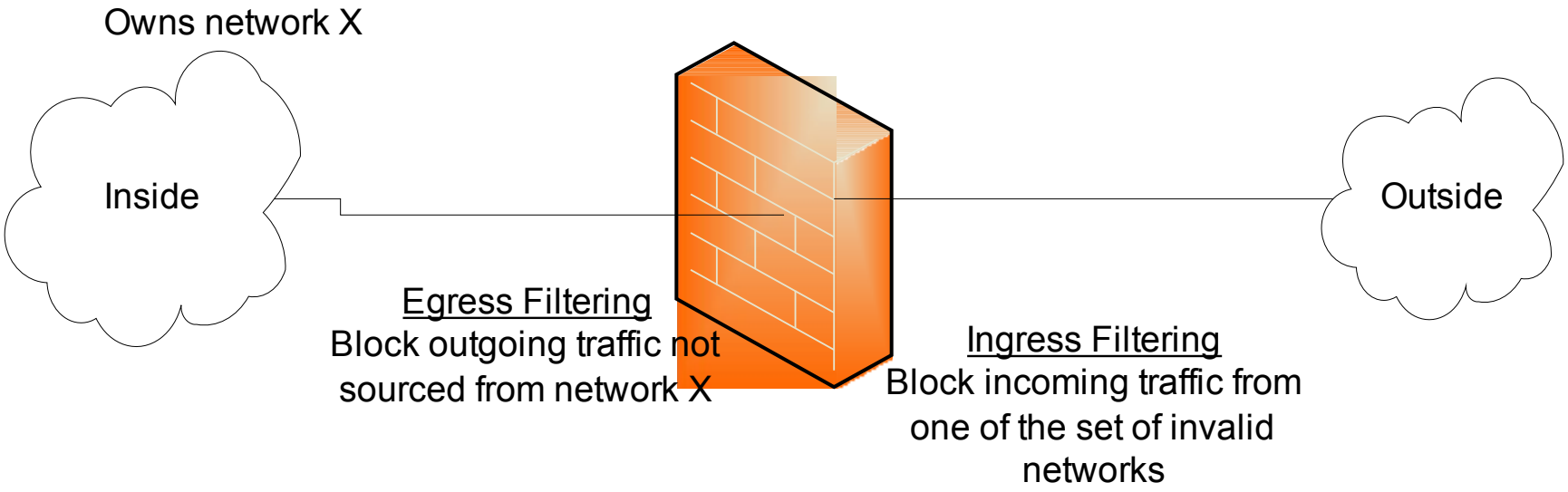
- Used to define traffic streams
  - Bind ACL's to interface and action
- Access Control Entry (ACE) contains
  - Source address
  - Destination Address
  - Protocol, e.g., IP, TCP, UDP, ICMP, GRE
  - Source Port
  - Destination Port
- ACL runtime lookup
  - Linear
  - N-dimensional tree lookup (PIX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

Inbound and Outbound ACLs

- On Cisco devices the ACL is bound to one interface
  - If traffic matches the ACL, associated action occurs
- ACL can interpret traffic as it enters the interface (inbound) or as it leaves the interface (outbound)
- Can have ACLs controlling on the same feature on both the incoming and outgoing interfaces

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



Activating Proxy control

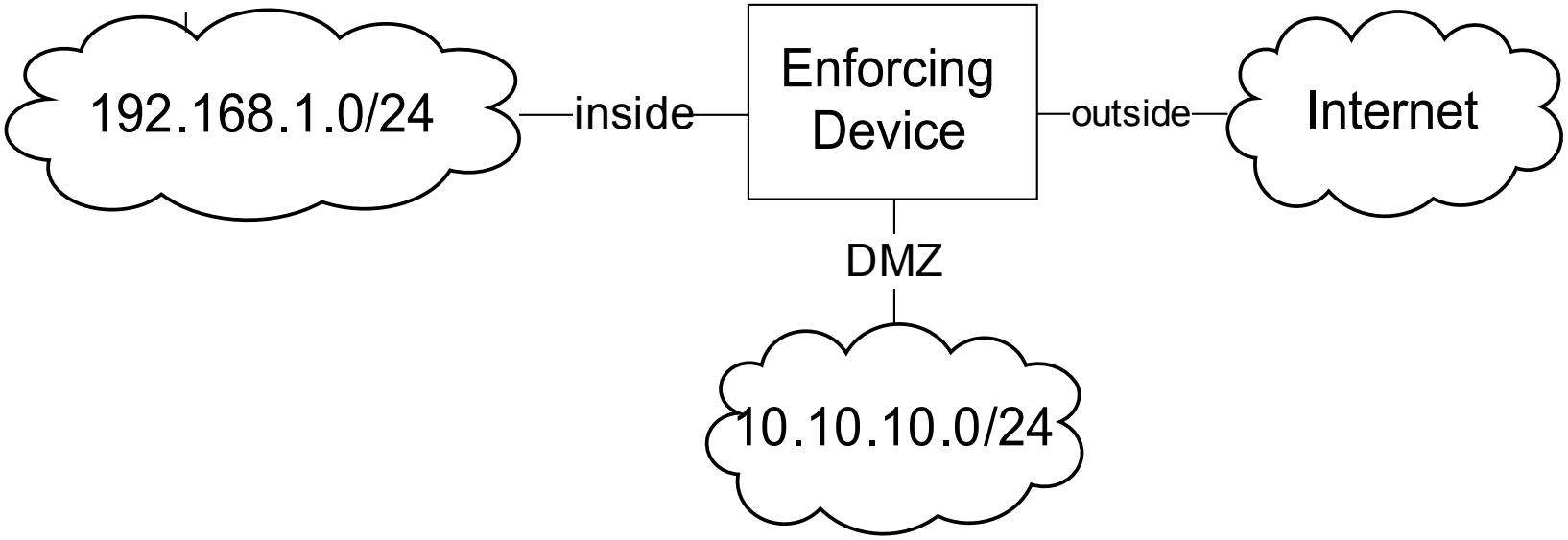
- A given firewall type has a fixed set of application proxies
- Configurations range on the granularity you can activate the proxies
  - Activate for all traffic with a particular destination port
  - Activate for traffic matching a particular ACL
  - Some proxies might be activated by default
- Activating a proxy will dynamically open holes for related protocol channels.

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
- 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

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

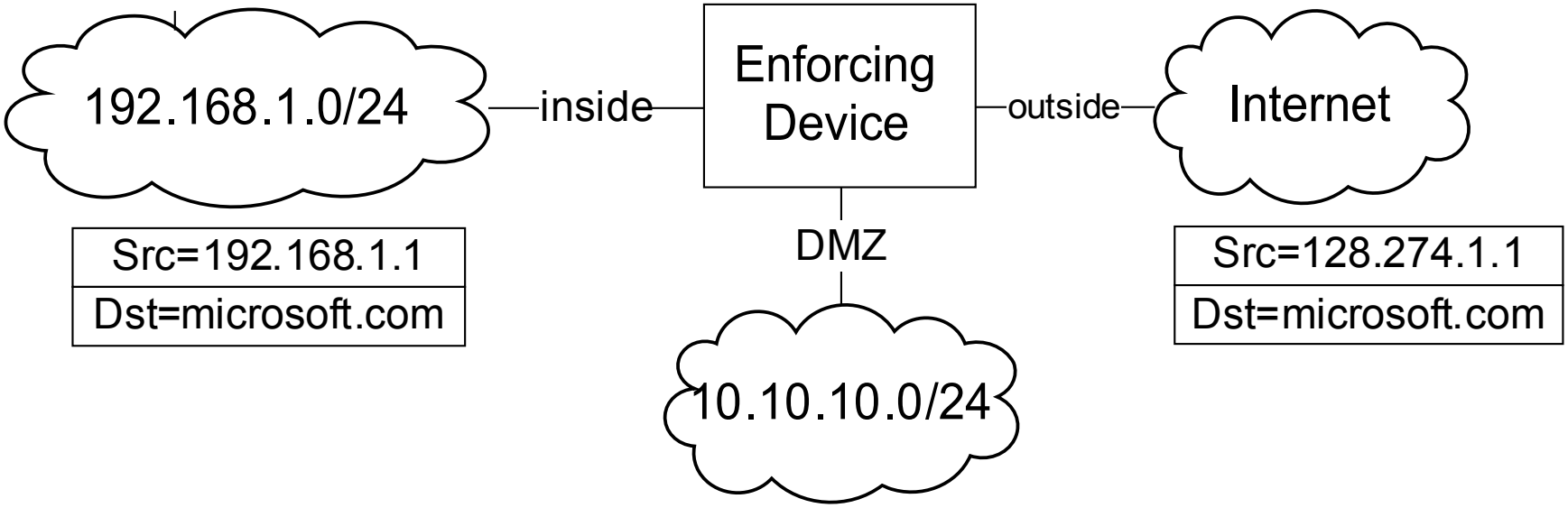


Address Hiding (NAPT)

- 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

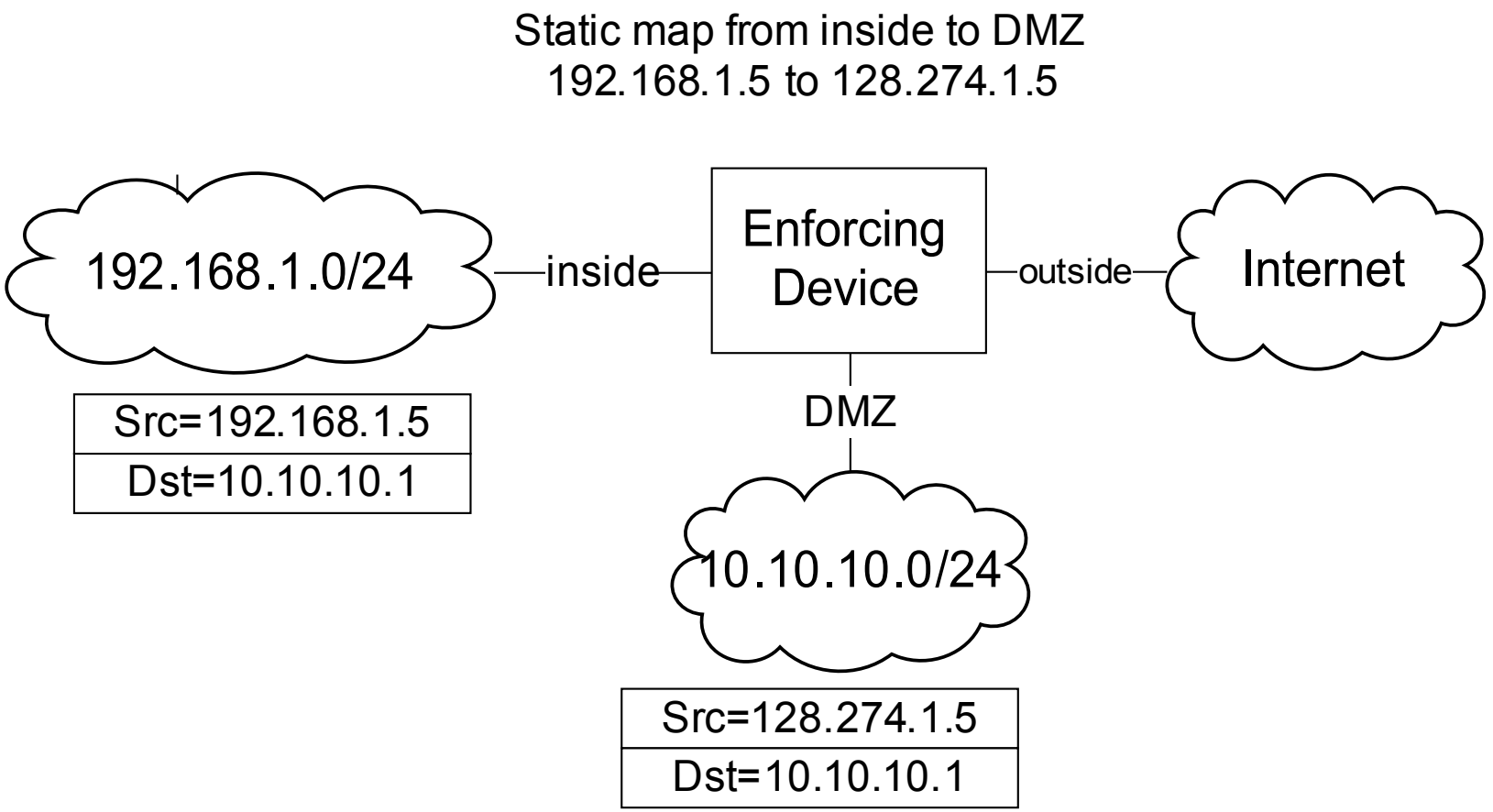
Hide from inside to outside
192.168.1.0/24 behind 128.274.1.1



Static 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

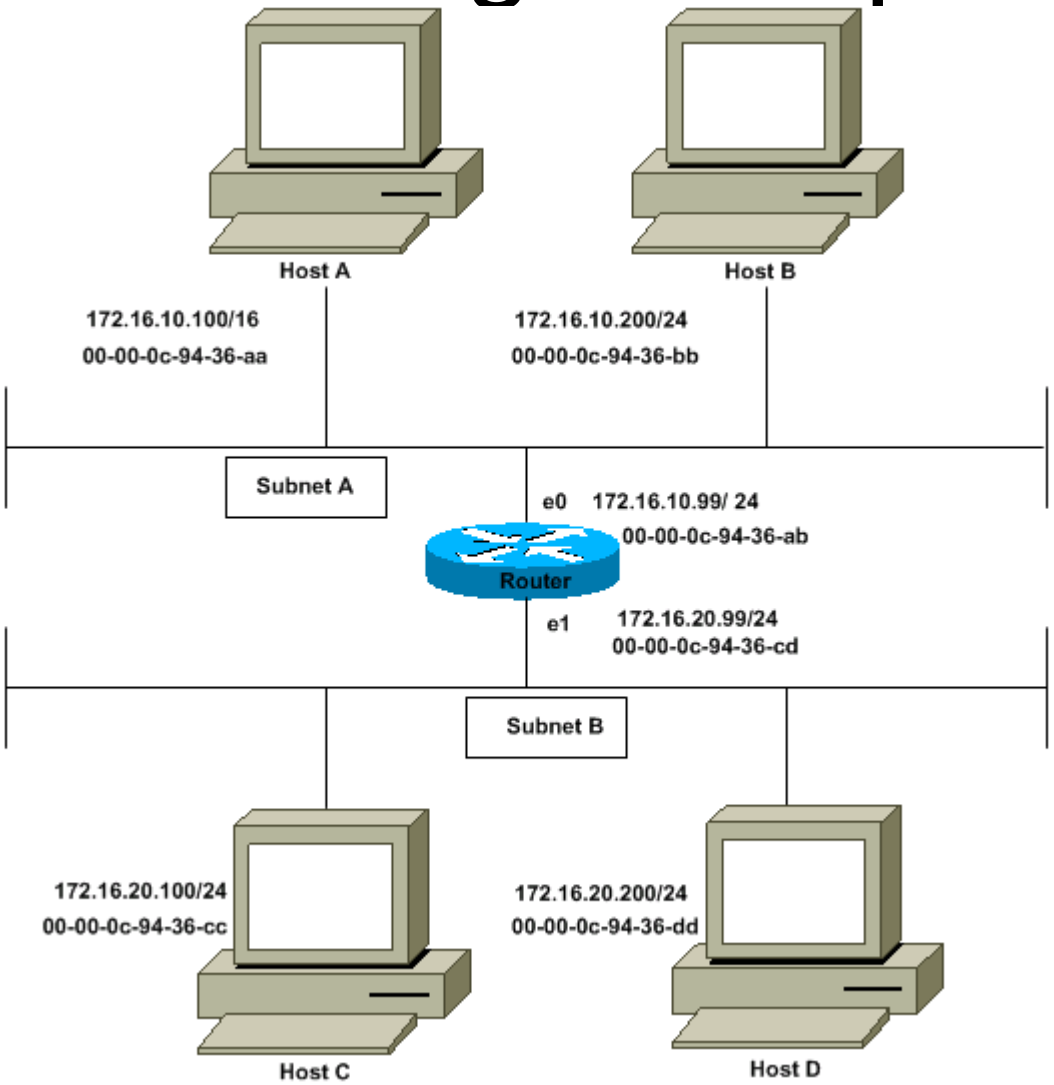
NAT example


Static map from inside to DMZ
192.168.1.5 to 128.274.1.5
192.168.1.0/24
inside
Enforcing Device
outside
Internet
DMZ
Src=192.168.1.5
Dst=10.10.10.1
10.10.10.0/24
Src=128.274.1.5
Dst=10.10.10.1

Proxy Arp

- Router Firewalls produces ARP replies for addresses “behind it”
  - http://www.cisco.com/en/US/tech/tk648/tk361/te
  - Goal to help with routing
- If misconfigured can bring down the network

Routing Example



Logging

- Syslog messages generated by firewalls
  - Logging frequency configurable to varying degrees
  - Messages sent on denied connections, permitted connections, translation events, etc.
- Syslog is UDP based, so logging message arrival not reliable
  - TCP syslog exists but never caught on
  - In the end must folks want the dropping to improve performance under stress
- Messages can be passed to multiple syslog servers
- Can be used for
  - Input to anomaly detectors
  - Forensics evidence

FW Runtime Characteristics

- Firewalls track streams of traffic
  - TCP streams are obvious
  - Creates pseudo UDP streams for UCP packets between the same addresses and ports that arrive near enough to each other
  - Stored in xlate table in PIX
  - conn_track in iptables
- Processing first packet in stream is more expensive
  - Must evaluate ACLs and calculate address translations
  - Subsequent packets get session data from a table

Point for other filtering

- If the firewall has reconstructed the traffic stream, can do other filtering
  - Filtering for “bad” URL’s
  - Virus Scan
  - Caching
  - IDS
  - Traffic ID

Multi-legged Firewalls

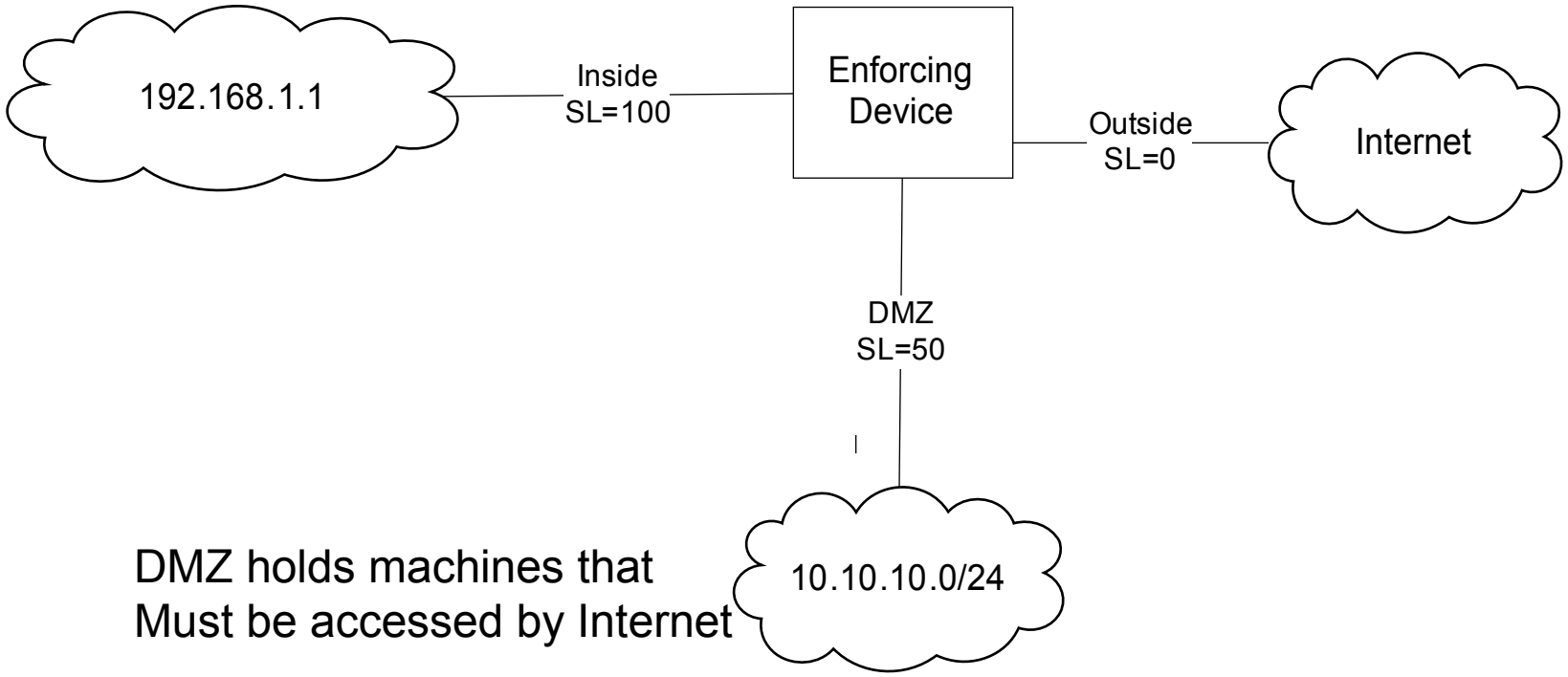
- Historically firewalls have protected inside from outside
  - Still true for the most part with personal and home firewalls
  - No longer sufficient for larger enterprises
- PIX security level solution
  - Outbound = traffic from low security level interface to high security level interface
  - Inbound = traffic from high security level interface to low security level interface
  - Different requirements for inbound and outbound traffic
- IOS divides interfaces into inside and outside groups
  - Address translation can only be defined between inside and outside groups
- Netscreens defines zones

PIX Inbound/Outbound Policies

- If not ACL's are present,
  - Outbound traffic is allowed
  - Inbound traffic is prohibited
- No traffic is allowed if the inside addresses are not translated
  - Source addresses of outbound traffic
  - Destination addresses of inbound traffic
- These default policies are evolving with newer PIX/ASA images

Classic Three Legged FW

Inside allows very limited if any
Incoming connections



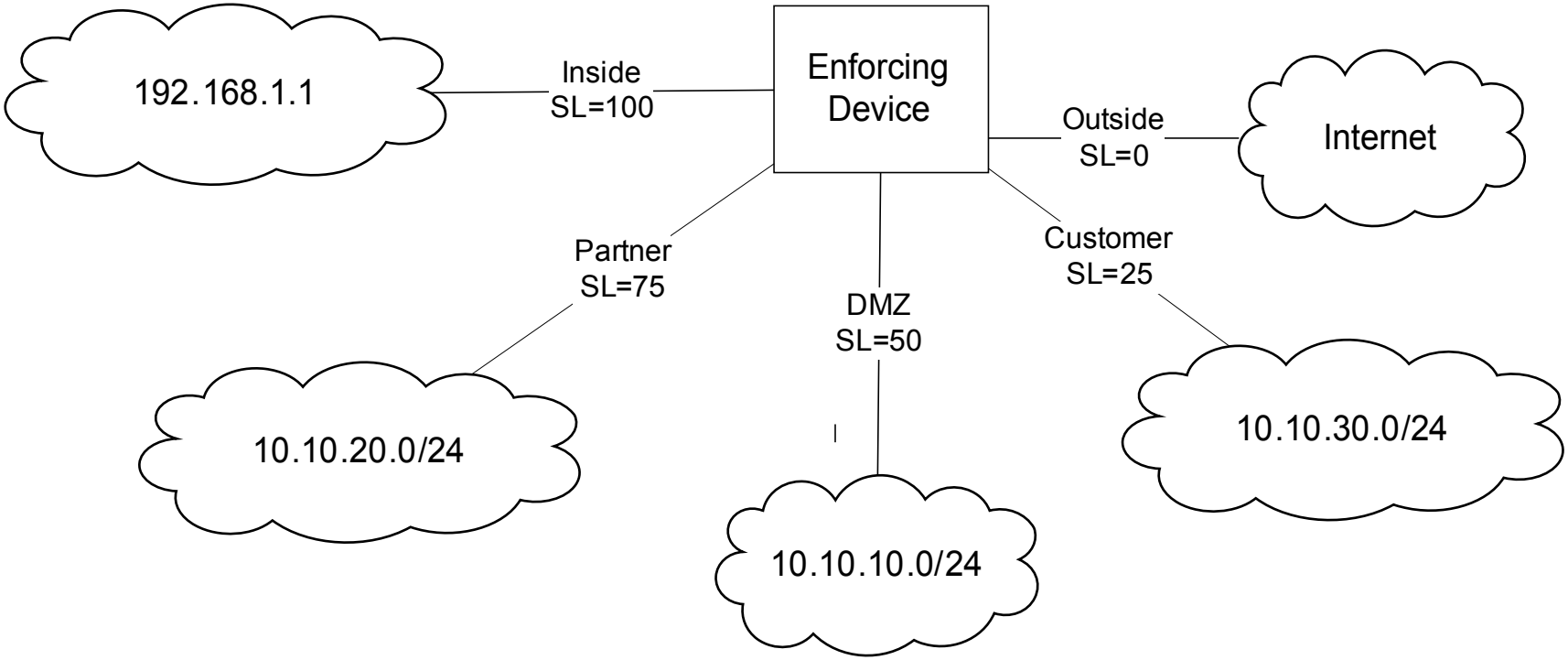
DMZ holds machines that
Must be accessed by Internet

Complications from Multiple Interfaces

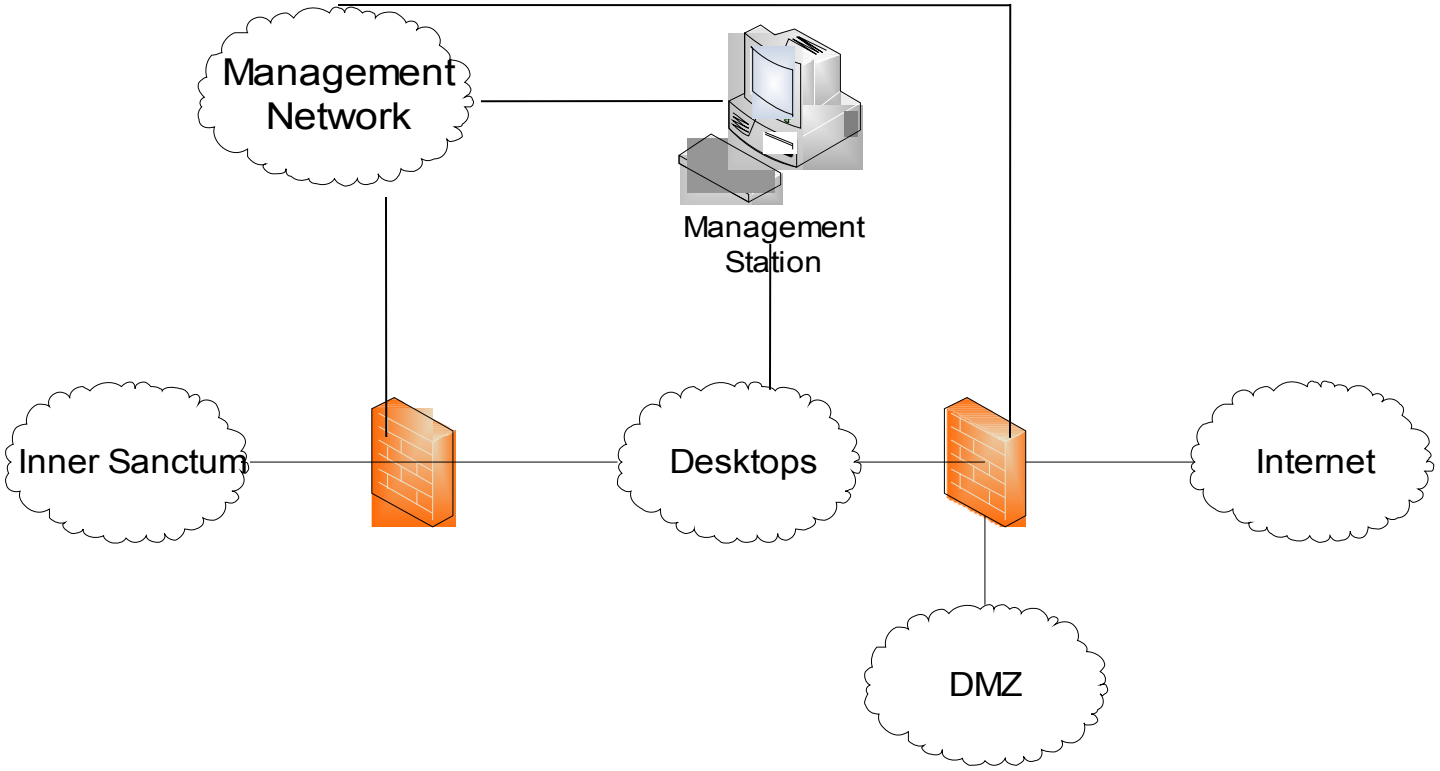
- Routing conflicts with address translation
  - Address translation specifies both interfaces
  - Must be evaluated before the routing, better be consistent
- Understanding traffic flows
  - Some firewalls have special rules for incoming vs outgoing traffic
  - Is traffic coming from Customer1 interface going to Customer2 interface “incoming” or “outgoing”?

Five Legged FW

- Static translation from DMZ to Customer
  - 10.10.10.10.1 to 128.1.1.1
- But routing table wants to route 128.1.1.1 from DMZ to outside interface
  - Static translation interface selection will win



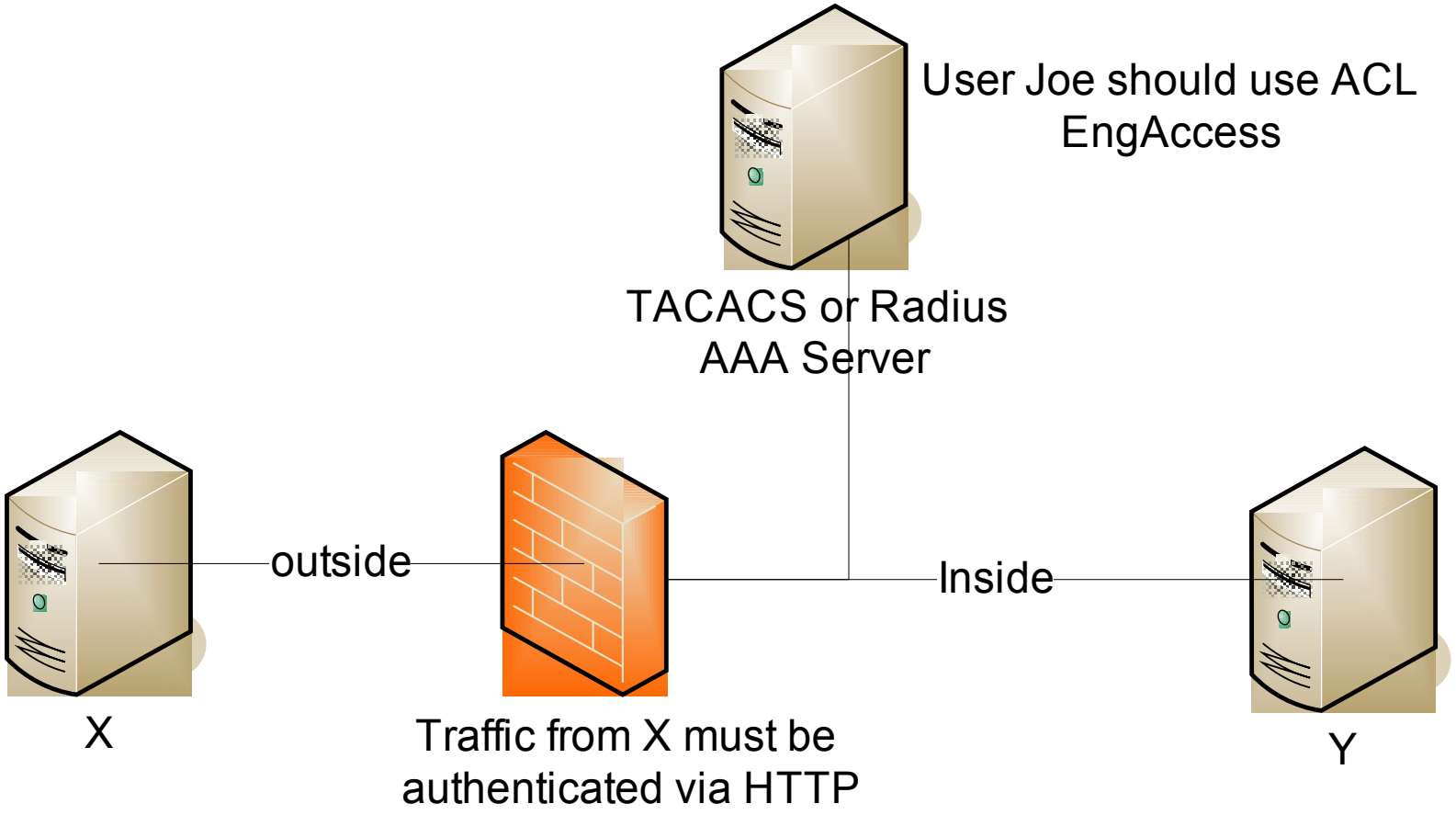
Out-of-band management



Identity Aware Firewall

- Use TACACS+ or Radius to authenticate, authorize, account for user with respect to FW
  - For administration of FW
  - For traffic passing through FW
    - PIX cut-through proxy allows authentication on one protocol to cover other protocols from same source
- Authorization for executing commands on the device
- Download or enable ACL's
- XAuth to integrate AAA with VPN authentication and other security mechanisms

AAA Scenario



Firewall Blades

- Following general HW trend to use blade cards to augment larger hardware platform
  - Firewall Service Module (FWSM) produced by Cisco
- In this case, blade card is inserted into a switch backplane
  - Leverage high bandwidth backplane
- With VLANs can have up to 100 interfaces
  - FWSM introduced mode that eliminates security level. Simplifies multi-legged interface configuration

Transparent Firewalls

- Layer 2 firewalls
  - Operates like a switch
  - Do not need to change the routing of your network
  - Each FW just has one IP address for management access
- Must ensure that all traffic passes through the firewall

Firewall Virtualization

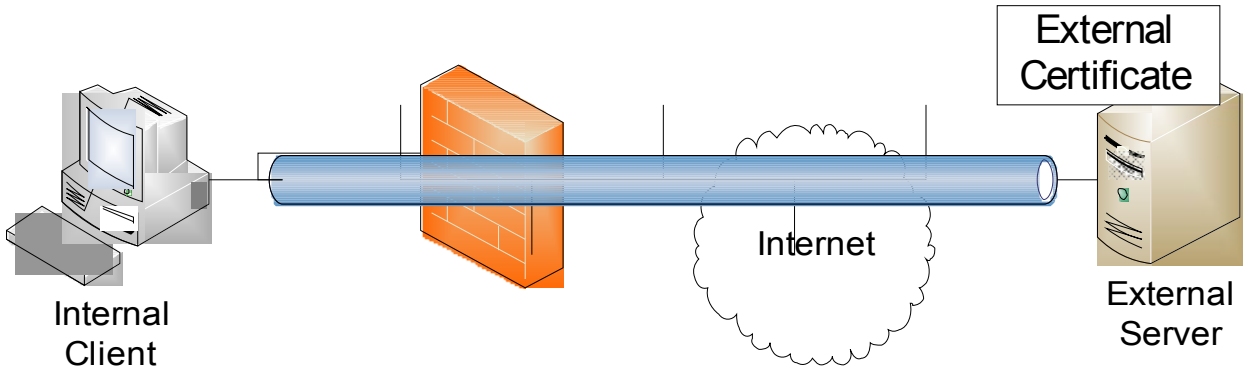
- One firewall supports 100's of virtual firewalls
  - Easier to provide separation with virtual firewalls than with one firewall with 100's of interfaces
  - Possible to separate administrative control

Is the Firewall Dead?

- Everything just tunnels through HTTP
- End-to-end security (encryption) renders firewalls useless
  - Tunnels hide information that firewalls would filter or sanitize
- Attacks change too quickly
- Blurring security domain perimeters
  - Who are you protecting from whom
  - Dynamic entities due to DHCP and laptops
  - More dynamic business arrangements, short term partnerships, outsourcing
- Total Cost of Ownership (TCO) is too high
  - Managing firewalls for a large network is expensive

Tunnels and Firewalls

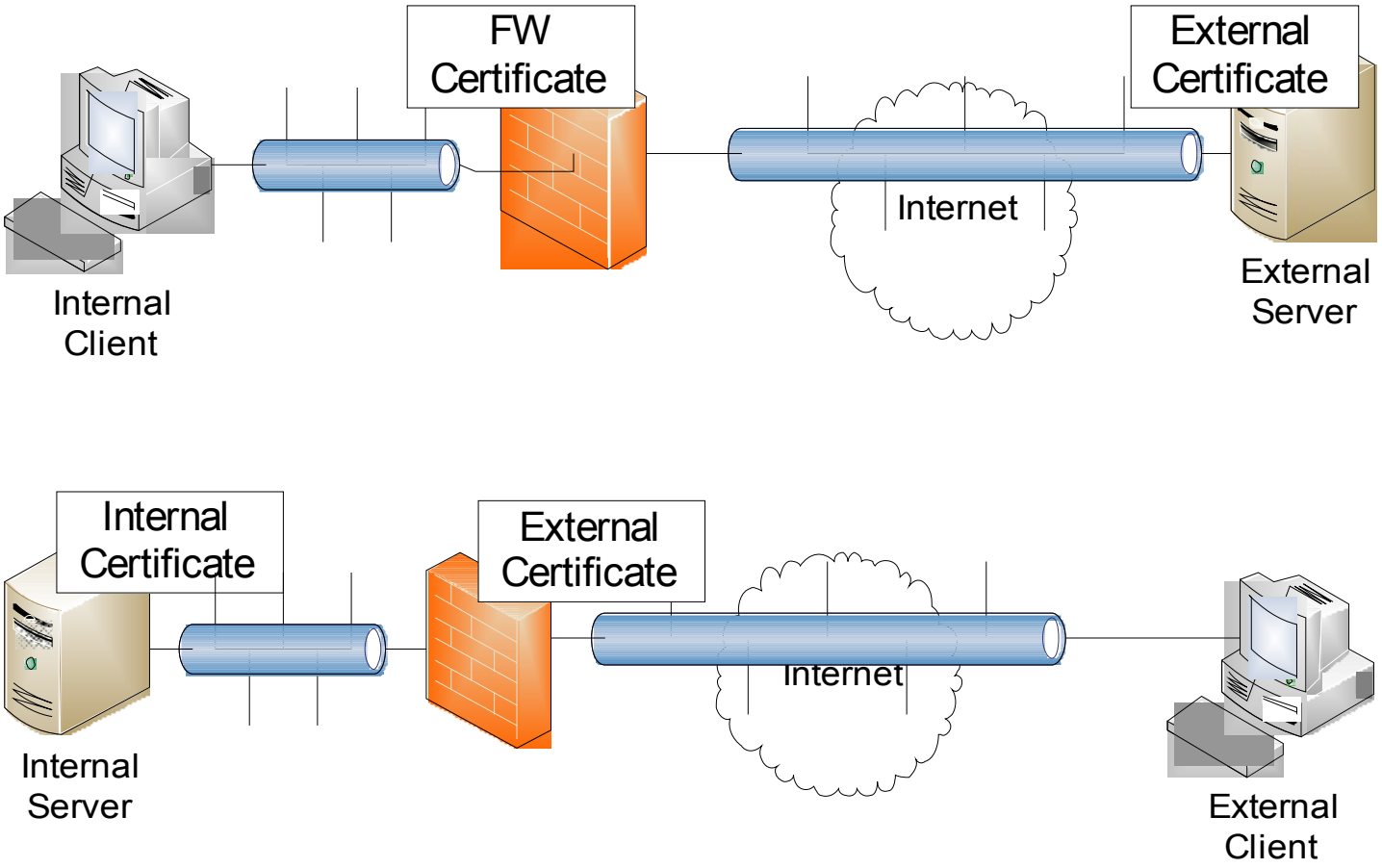
- Firewalls cannot look into tunneled traffic
- At most can do some header filtering
  - Can tunnel many protocols through HTTP



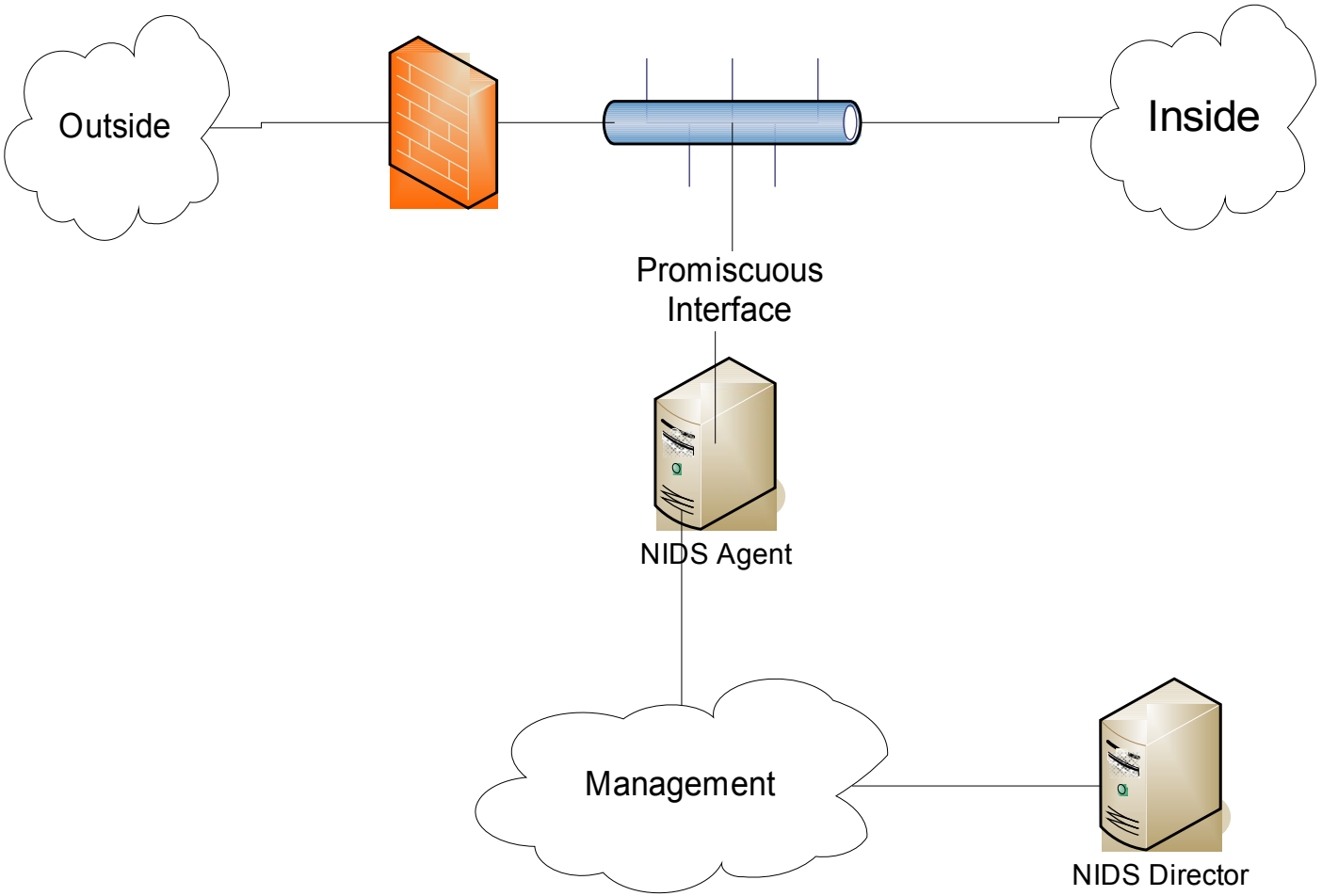
Tapping SSL Tunnels

- Offered by Palo Alto Networks and Netronome (at least)
  - Proxy the tunnel
  - Create tunnel from client to FW
  - Create another tunnel from FW to server
- Dealing with certificates can be tricky

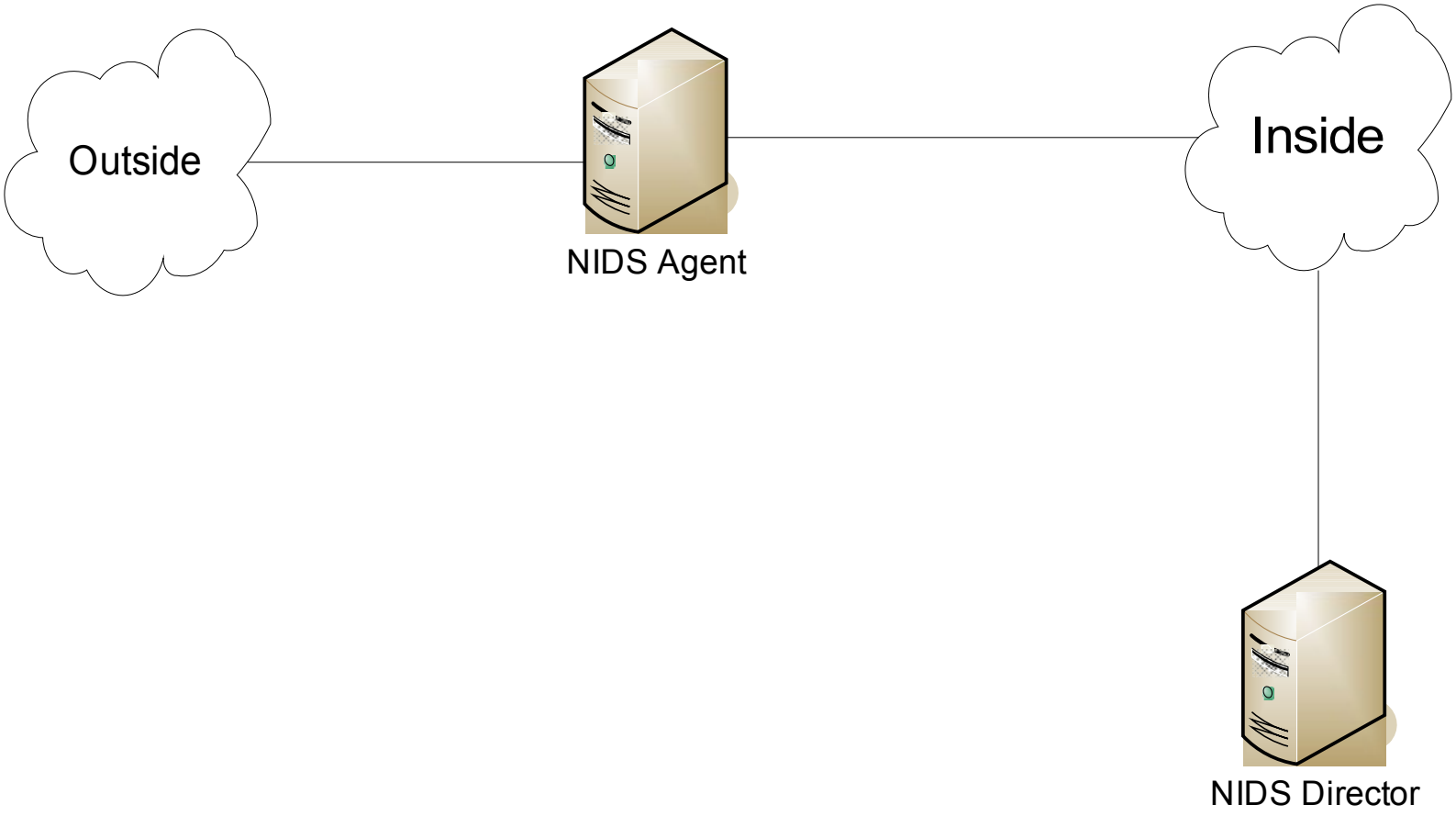
Two SSL Tapping Cases



Classical Network Intrusion Detection (NIDS) deployment



Network Intrusion Prevention System (IPS) scenario



One Example of IPS/FW Fusion

- Dynamically detecting application protocol
- Many apps tunnel through HTTP
  - In traditional FW cannot block or filter these apps differently than HTTP
- Palo Alto Networks and SourceFire offer application signatures
  - E.g. Skype or AIM signatures

Distributed Firewall Instead?

- "Implementing a Distributed Firewall" http://www1.cs.columbia.edu/~angelos/Papers/df.pdf
- The actual firewalls are on each client and server machine
  - End-to-end security
- Still has management cost issues.
- Some sort of centralized control is necessary to maintain some semblance of a security policy
  - Call home protocols
  - Security profiles
- Could have a subversive client
  - Would need to dynamically verify health and stance of booting/attaching system

Another alternative

- Network Admission Control (NAC)/Network Access Protection (NAP)
  - http://www.cisco.com/en/US/netsol/ns617/networking_
- Enforcement remains in the network but knowledge of endpoint is added
  - Requires software on the client to communicate client state to enforcement device
  - New client to enforcing device protocol. Must detect subversive clients
  - Must ensure that this software runs on all clients (like VPN software now)
- Enforcement devices uses TACACS to query AAA Server about policy that applies to client profile.

The Firewall Future

- Firewall technology will continue to change
  - Increased operational change
    - Dynamically react to newly discovered “bad” machines
  - More user aware
  - Increased role of endpoint machines, but centralized firewalls provide layered security
  - IPv6 roll out may leverage firewalls as quick fix points
- Integration with other technologies
  - Intrusion detection
  - Other scouring technologies
  - Encryption/authentication
- Obsoleted by some technologies
  - End-to-end encryption – only basic filtering can be done