IT-ADVENTURES

MAKING IT FUN

Networking Administration

Module 7

Network Component Review

- NIC – Network Interface Card – transceiver that allows a computer to transmit and receive information with other devices
- Bridge – Layer 2 device – Not in use much, but conceptually it joined two networks and repeated traffic destined to the adjacent network

Network Component Review

- Hub – Layer 2 – physically terminates multiple twisted pair cables in a common device and provides a common communications channel for attached devices.
  - Every device hears every other device
- Switch – Layer 2 – physically terminates multiple twisted pair cables in a common device and provides a private channel with each connected device. Allows devices to communicate with other attached devices by repeating traffic to only the attached destination device.

Network Component Review

- Router – Layer 3 – Forwards received IP packets to one of its NICs based on the subnet of the destination and routing rules.

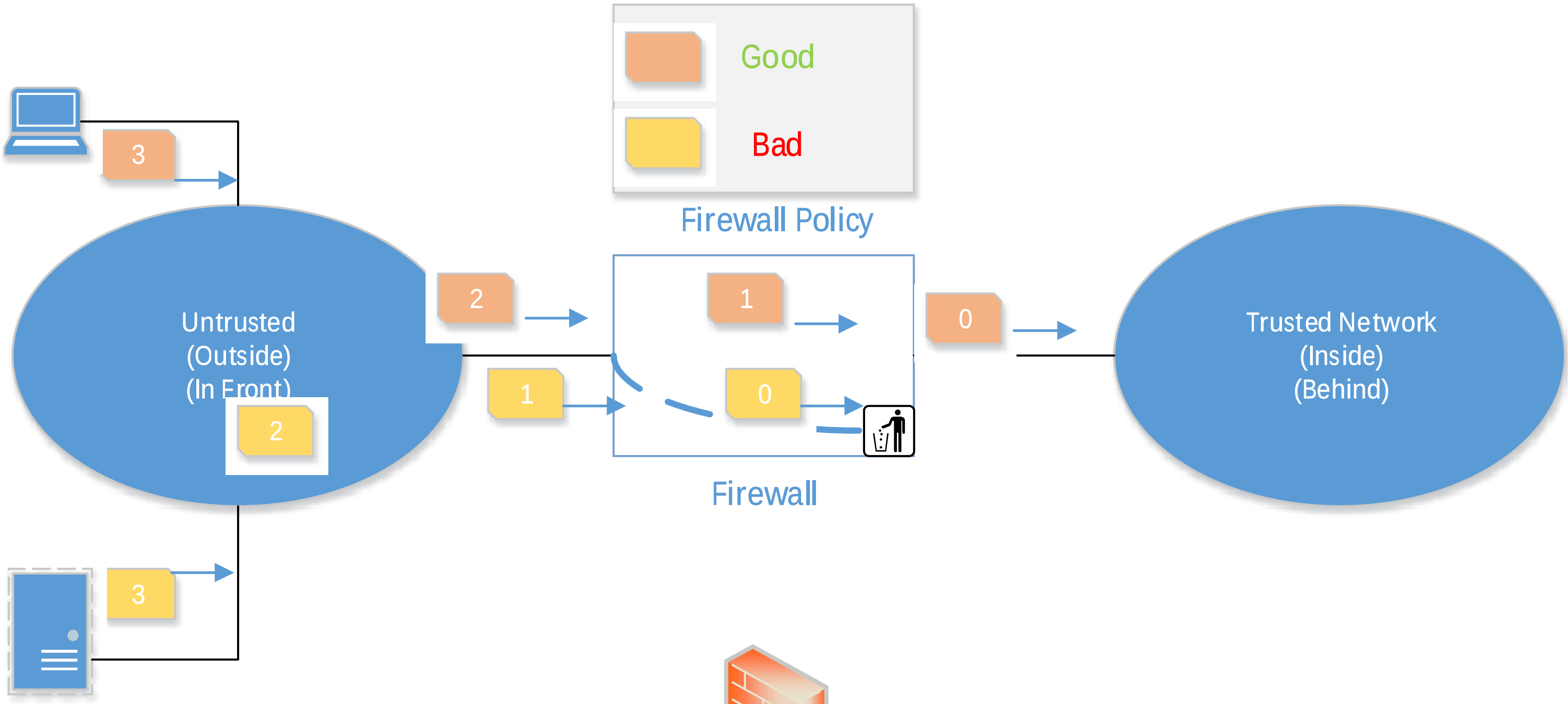
Firewalls

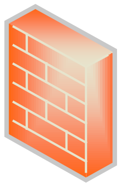
- Purpose – Limit the network exposure of systems behind it from the network on its untrusted side – commonly the Internet.
- Firewalls are Layer 3 or Layer 7 devices
  - High Bandwidth connections are protected by Layer 3 devices
- Firewalls can be attached to multiple networks
  - Firewall attempts to restrict access to each network

Firewalls

- Layer 3 - Functionality – Inspects packets and allows those that match rules (firewall policy) and discards everything else
  - Allowed packets are forwarded to the correct interface on the firewall – like a router
  - Stateful inspection means that the firewall understands protocols with state like TCP
    - The initiating "syn packet" will be denied as well as all the following packets related to the desired but denied session

Firewalls





Common Firewall Symbol

Firewalls

- Layer 7 – Proxy Firewalls – Functionality
  - Secured computer running tiny reliable programs that intercept connections.
  - Connection is made with proxy by client and proxy makes new connection with destination
  - Proxy enforces protocol
  - Proxy policy rules can be sensitive to protocol and potentially content
  - Some proxy firewalls have Layer 3 features

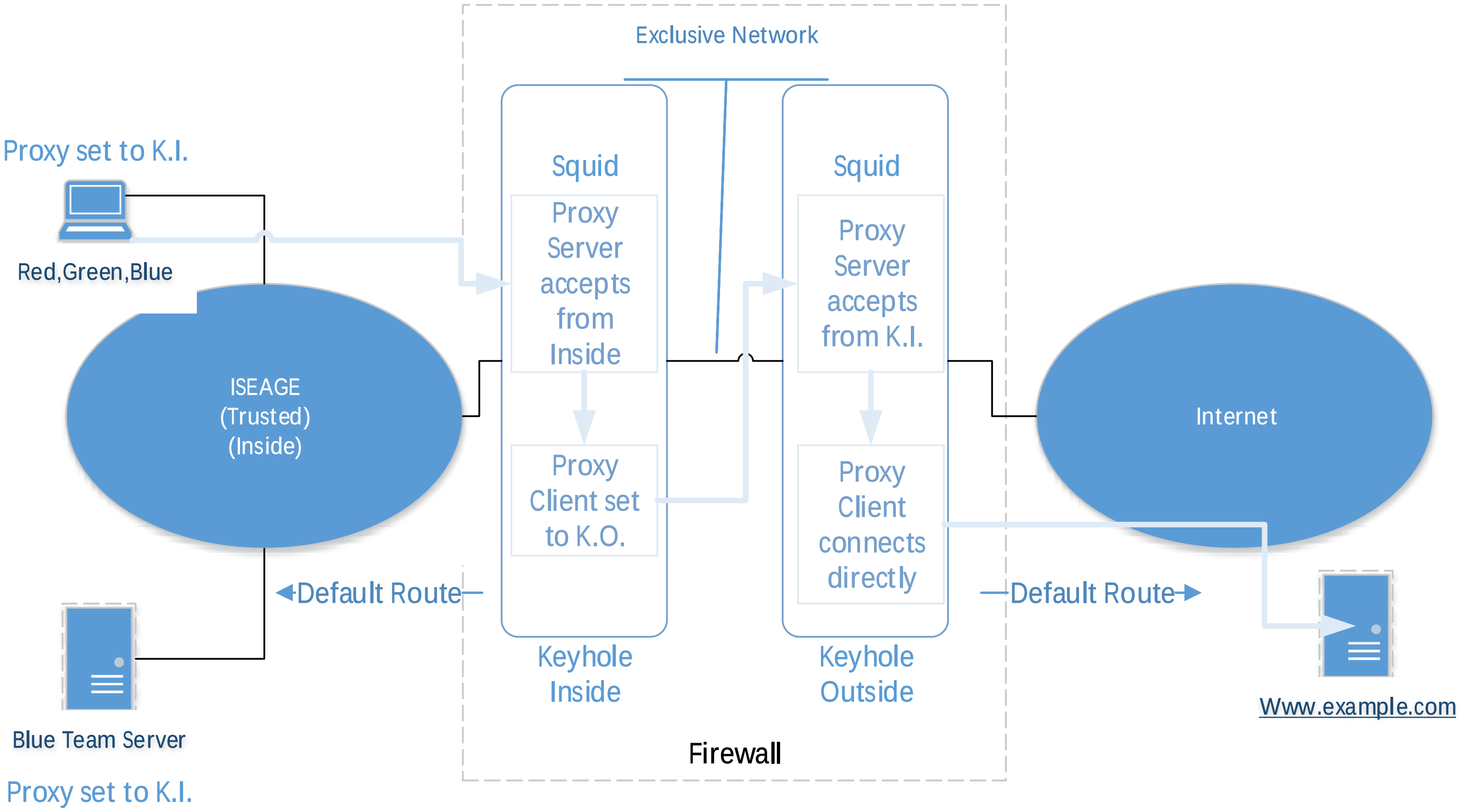
Firewalls

- Routers can be configured to be Layer 3 firewalls with ACLs
- Specialized software or devices are trusted more
  - Pfsense, Layer 3, will be used by you
  - Keyhole in playground is a proxy firewall
  - Cisco, Checkpoint are big commercial vendors

Firewalls are "Trouble"

- Correct use of firewalls requires all traffic to pass through them
- Network problems experienced by other administrators and users are commonly blamed on firewalls
  - Sometimes they are right
  - A better understanding of application may avoid firewall problems or false claims
    - Adjust firewall rules with correct information

ISEAGE Firewall



Routing

- Terms for router roles:
  - Adjacent router – Network attached to router contains either source or destination of traffic
  - Intermediate router – Traffic being forwarded by the router will be delivered to another router
- Needed when connecting two more IP networks together
  - Router typically has one or more NICs
  - Common to dedicate a NIC for each adjacent IP network
    - VLANs make it possible for more nets per NIC (advanced topic)

IP Netmask Review

IP Address	Netmask	Network Address	Host Address
10.15.16.17	255.0.0.0 = /8	10.0.0.0	15.16.17
10.200.5.87	255.255.255.0 = /24	10.200.5.0	87
129.64.87.145	255.255.0.0 = /16	129.64.0.0	87.145
191.36.72.48	255.255.255.128 = /25	191.36.72.0	48
191.36.72.148	255.255.255.128 = /25	191.36.72.128	20
191.36.72.48	255.255.255.192 = /26	191.36.72.0	48
191.36.72.148	255.255.255.192 = /26	191.36.72.128	20
191.36.72.48	255.255.255.224 = /27	191.36.72.32	16
191.36.72.148	255.255.255.224 = /27	191.36.72.128	20
191.36.72.48	255.255.255.240 = /28	191.36.72.48	0
191.36.72.148	255.255.255.240 = /28	191.36.72.144	4

IP Netmask Review

IP Address

191. 36. 72. 48

1011 1111.0010 0100.0100 1000.0011 0000

Address 1011 1111.0010 0100.0100 1000.0011 0000

Mask

1111 1111.1111 1111.1111 1111.1000 0000
1111 1111.1111 1111.1111 1111.1100 0000
1111 1111.1111 1111.1111 1111.1110 0000
1111 1111.1111 1111.1111 1111.1111 0000
1111 1111.1111 1111.1111 1111.1111 1000
1111 1111.1111 1111.1111 1111.1111 1100
1111 1111.1111 1111.1111 1111.1111 1110
1111 1111.1111 1111.1111 1111.1111 1111

AND

Network Address

191. 36. 72. ??

1011 1111.0010 0100.0100 1000.0000 0000 = 0
1011 1111.0010 0100.0100 1000.0000 0000 = 0
1011 1111.0010 0100.0100 1000.0010 0000 = 16
1011 1111.0010 0100.0100 1000.0011 0000 = 48
1011 1111.0010 0100.0100 1000.0011 0000 = 48
1011 1111.0010 0100.0100 1000.0011 0000 = 48
1011 1111.0010 0100.0100 1000.0011 0000 = 48
1011 1111.0010 0100.0100 1000.0011 0000 = 48

Routing

- Router knows from its rules if packet is destined to adjacent network
  - If so, packet is delivered “locally”
  - Router ARPs for destination device’s MAC address and sends frame to correct NIC
- Routing rules needed for forwarding
  - Most common is Default Route
    - If no existing rules instructs otherwise, packet is forwarded to default router
    - Router ARPs for next router’s MAC address and sends frame to correct NIC

Routing Rules

- Many OS types recognize adjacent networks and automatically configure router rules for them
- Routing rules can be for network or a specific host
    - Network routes are most frequently configured
    - Rules consist of : Destination type, destination, gateway/router, netmask

Routing Rules Management

- Large networks
  - Routing protocols are used to automatically configure routing tables on routers
    - Helpful when new networks are created and old networks are removed
    - Helpful when connectivity between routers has problems
      - Alternative routes are determined
    - RIP, OSPF are some intranet protocols (advanced topic)
    - BGP is used on Internet routers (advanced topic)

Routing Rules Management

- Small stable networks
  - Routing protocols are not needed
  - Routing protocols can be complicated
  - Manual routing configuration is simpler
    - If multiple paths exist between internal destinations and sources, dynamic routing protocols might be helpful.
  - Manual routing is more secure
    - Routing protocols can be manipulated and can result in paths between devices being used or avoided although better path options exist.
    - Trust can result in routers being convinced to flow traffic through a compromised device allows for packet capture and analysis – source of secrets loss

Firewalls and Routing

- Layer 3 and Layer 7 firewalls require each interface to be on different IP subnets
  - Routing function occurs after decision to pass traffic
  - Broken routing may cause firewall troubles, so a problem may not be with firewall rules
  - Don’t forget the firewall’s routing tables
- Getting the Inside and Outside interfaces switched around can also break connectivity
    - Normally happens during firewall installation and initial configuration

Tunneling

- Sending network traffic in a form that firewalls, routers and other network devices may not recognize its true nature or purpose.
- The recipient will need to know how to process the tunneled traffic
- Legitimate purposes:
  - Proxy connections
  - Network traffic encryption

Tunneling

- Not so legitimate:
  - – Playing multi-player video games over the HTTP port (TCP port 80)
  - – Malware calling home over commonly permitted ports.

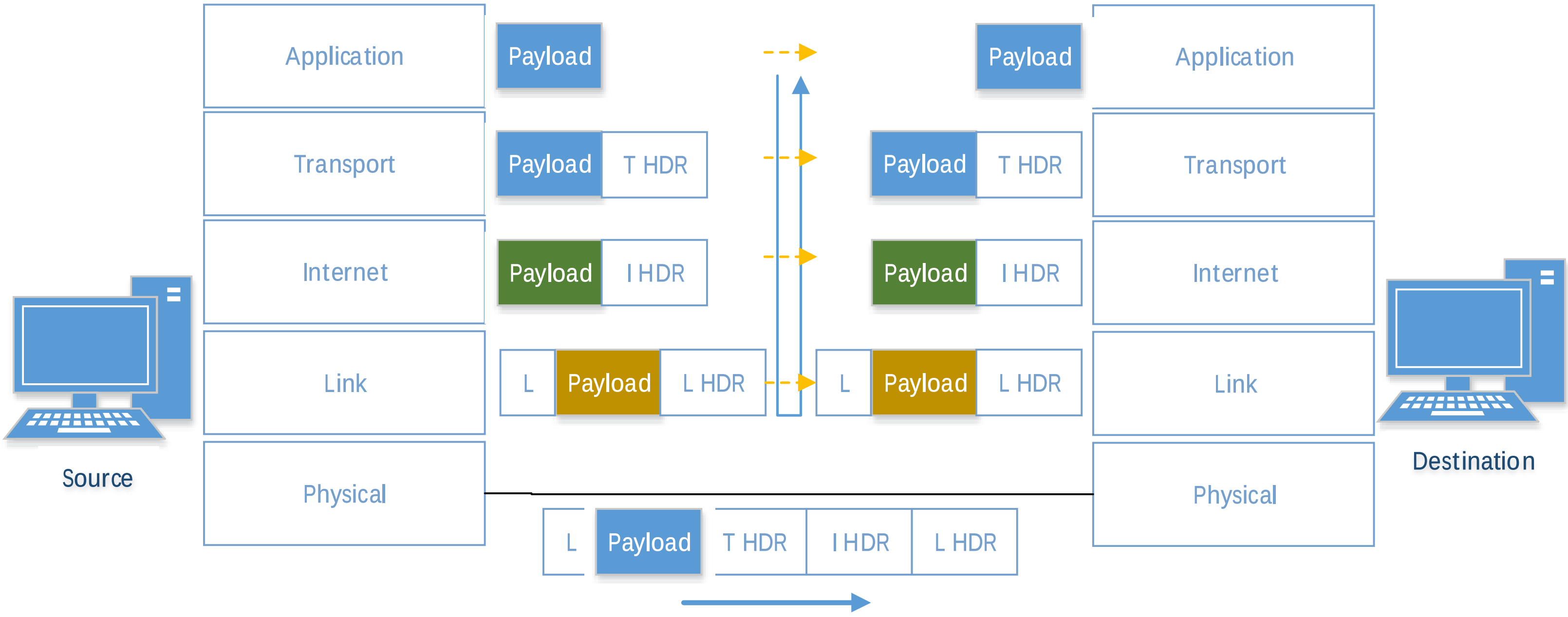
Tunneling

- How does it work?
  - – Network protocol stack design implements the concept of encapsulation
  - – Each protocol layer has functions to perform on received and soon to be transmitted data
  - – Each protocol layer is logically interacting with its peer layer on the destination
  - – These interactions require sharing information
  - – The to data the user desires to transmit is the “payload”

Encapsulation

- As the payload is passed down the stack to the point of physical transmission, each layer attaches its necessary pieces of information
- After the last layer adds its pieces of information it is transmitted
- The destination's stack will interpret the appropriate piece and strip it off before passing the received information higher

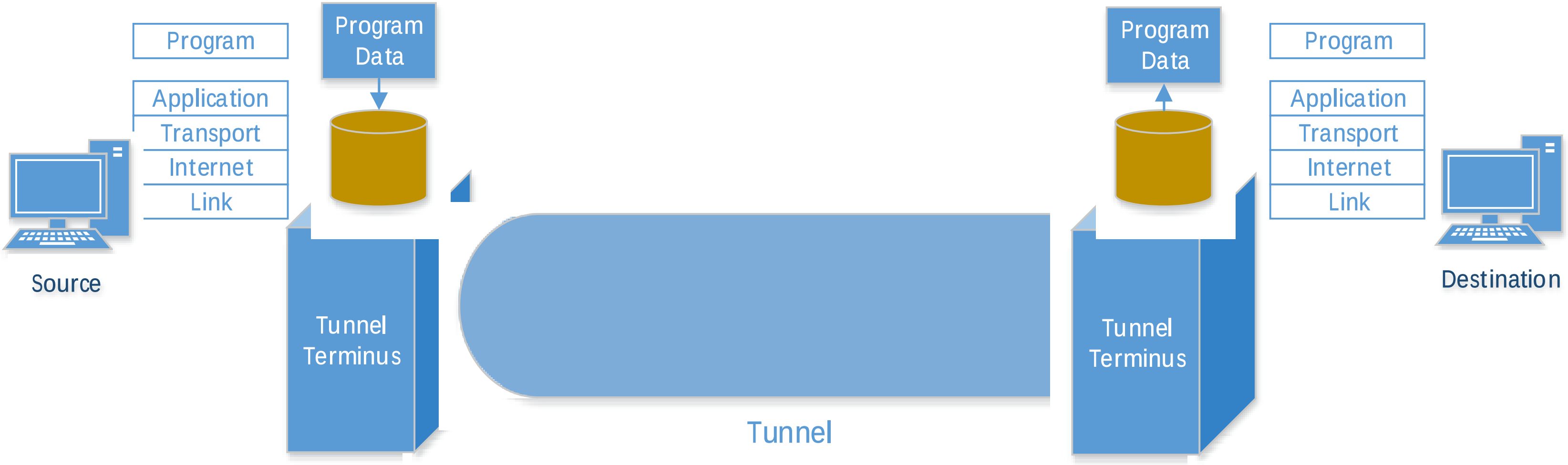
Encapsulation



Copyright 2013 Iowa State University

Tunneling

- The process of each layer contributing its information and the receiver's peer layers stripping if off is called encapsulation.
- Tunneling takes advantage of this activity



Proxied Connections

- Keyhole supports HTTP, HTTPs and FTP
- Many browsers understand proxied connections
  - Browser makes an HTTP connection to proxy
  - In the payload is the entire URL, so proxy knows target server
    - Normally browser makes direct HTTP connection to server and only passes path to content to server – server info is redundant to server
    - Proxy makes connection like browser to server

Proxied Connection

- Proxy passes page request information to server and receives reply
- Proxy passes reply back to browser
- But, in ISEAGE two proxies are needed.
  - The inside proxy knows about the outside proxy
  - It makes a new proxied connection and forwards the URL to the outside proxy.

Proxied Connection

- ISEAGE behaves like the Internet
  - All IP address are treated as internal to ISEAGE
    - Why route an IP address anywhere beyond immediate reach?
  - Contact to the true holder of an IP address requires the connection to tunnel to a known ISEAGE routed and reachable address
    - Once passed though all of ISEAGE routing, the proxy knows how to get to the real server on the Internet

Proxied Connection

- FTP proxing is even fancier tunneling
  - Browser makes HTTP connection to proxy with FTP URL using HTTP commands
  - Assuming only one proxy, proxy issues FTP connection and uses FTP commands
  - Directory listings and file content is passed to proxy via FTP
  - Proxy translates FTP content for browser using HTTP and HTML
  - Browser processes the HTTP content

Encrypting tunnels

- They can occur at any layer in stack
  - Point-to-point (HTTP+SSL/TLS, SSH, RDP)
  - Point-to-Network (SSL, IPSEC, IPv6)
  - Net-to-Net (IPSEC,IPv6)
- Virtual Private Networks (VPNs) use centralized network devices
- Traffic before and after tunnel terminus is not encrypted
  - Big e-commerce sites use specialized SSL devices and pass traffic to WWW server in the clear

Encrypting Tunnels

- SSL/TLS can be used to tunnel any TCP enabled protocol
  - Practical, so long there is tunnel terminus on the client and server side.
- IPSEC for IPv4 and IPv6 create tunnels at the Internet (IP) layer.
  - The potential is to encrypt any IP related protocol (ICMP, TCP, UDP, etc.)

Private Address Ranges

- The IPv4 address space is smaller than current Internet needs
  - But, big enough for any one organization
- To stretch out the usefulness of IPv4 addressing, some addresses are reserved as private
  - Internet routers do not have routing rules to forward packets to private addresses
    - Some have rules to discard related packets

Private Address Ranges

- Private addresses used within organizations
- Communication to or from the organization over Internet requires non-private, scarce, routable addresses
- Private Address Ranges
  - 10.0.0.0 – 10.255.255.255 – Class A
  - 172.16.0.0 – 172.31.255.255 – 16 Class B's
  - 192.168.0.0 – 192.168.255.255 – 256 Class C's

Network Address Translation

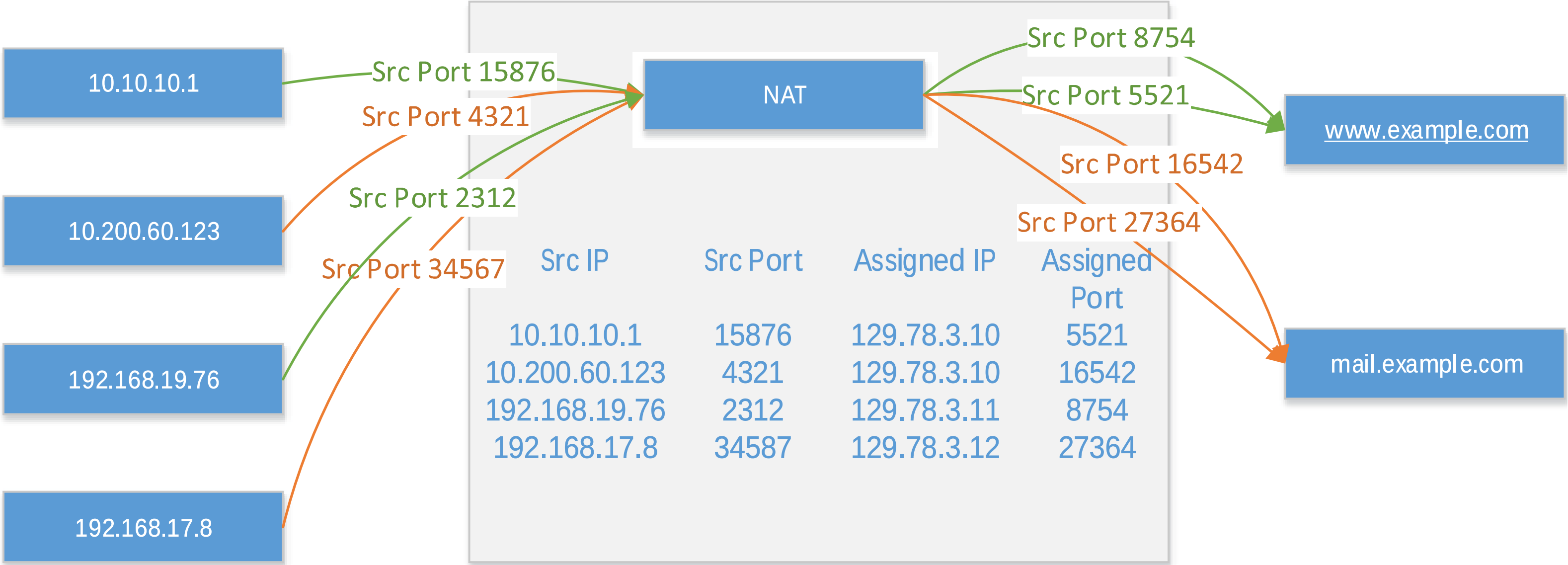
- How does a PC with 172.16.12.45 get packets to and from to www.google.com?
  - With a device that replaces the source 172.16.12.45 address with a routable address
  - Received packets for original requestor are adjusted so the destination address is 172.16.12.45, which the org.'s internal network and PC recognize

Network Address Translation

- There are hundreds of internal devices in organization, do we need hundreds of routable addresses?
  - No. Connections from networked devices typically use protocols that use TCP or UDP
    - Client address and port saved in a table with translated address and new client port
    - Received packets are matched in the table, so more than one device or connection can be mapped to one routable address

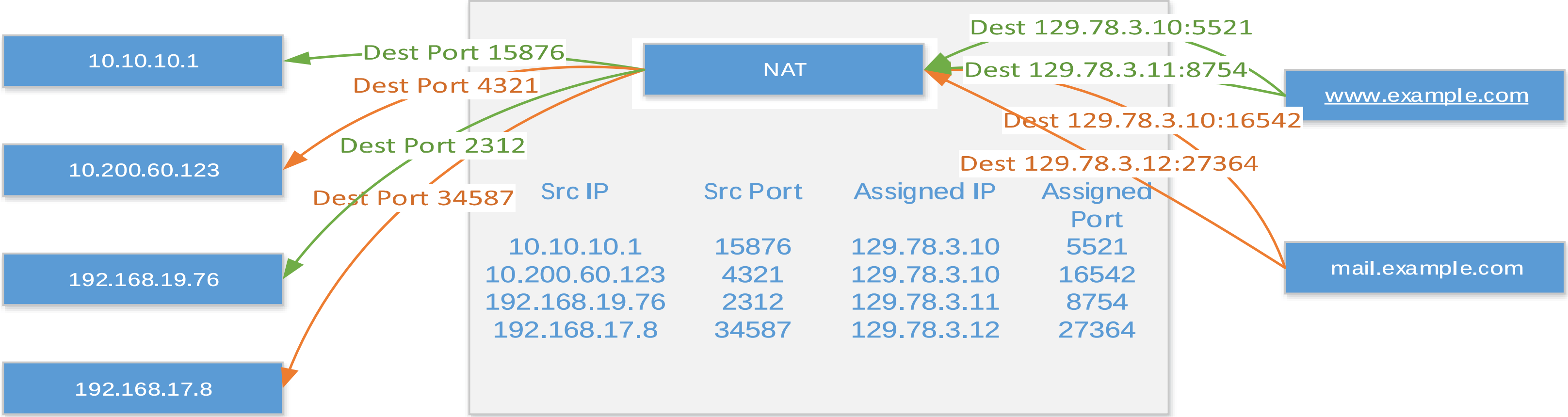
Network Address Translation

- Static NAT
  - Allows a server configured with private address to be consistently accessed by Internet clients on same address
    - There is a 1:1 mapping of addresses



Src IP	Src Port	Assigned IP	Assigned Port
10.10.10.1	15876	129.78.3.10	5521
10.200.60.123	4321	129.78.3.10	16542
192.168.19.76	2312	129.78.3.11	8754
192.168.17.8	34587	129.78.3.12	27364

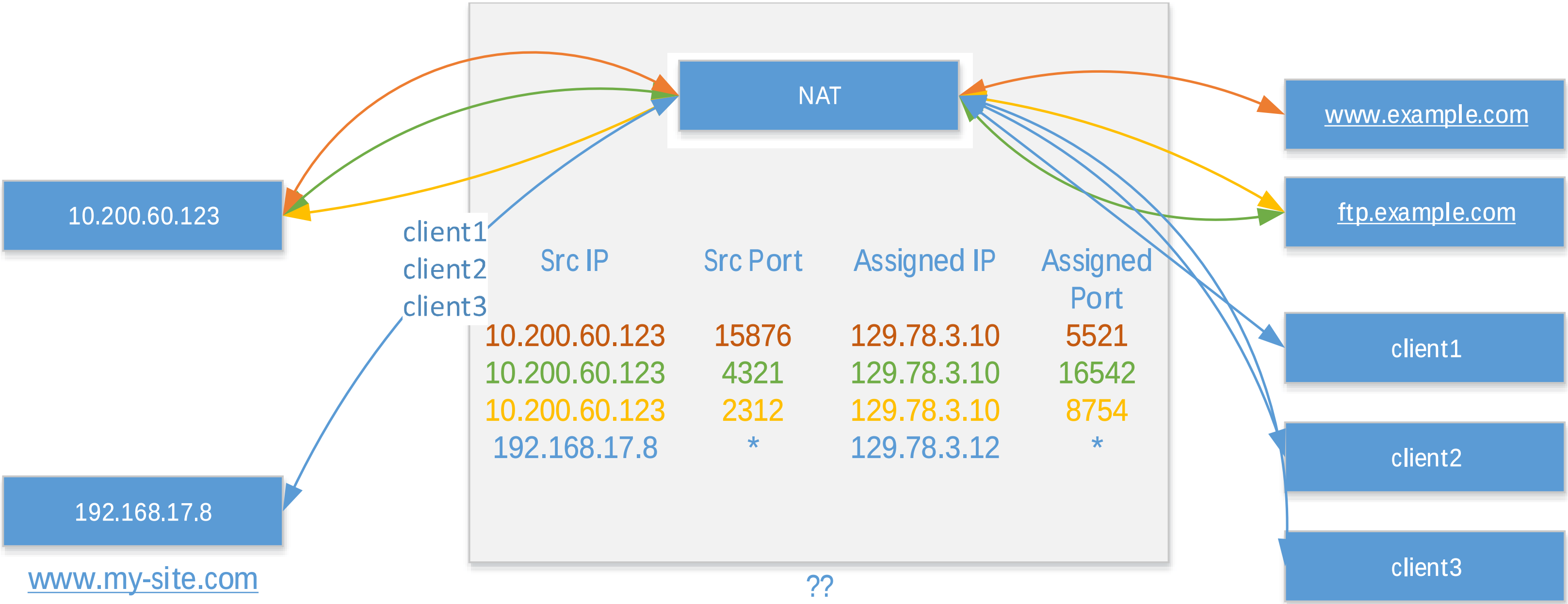
Client Request Packets Sent to Internet Servers



Src IP	Src Port	Assigned IP	Assigned Port
10.10.10.1	15876	129.78.3.10	5521
10.200.60.123	4321	129.78.3.10	16542
192.168.19.76	2312	129.78.3.11	8754
192.168.17.8	34587	129.78.3.12	27364

Server Reply Packets Delivered to Clients

Dynamic and Static NAT



Src IP	Src Port	Assigned IP	Assigned Port
10.200.60.123	15876	129.78.3.10	5521
10.200.60.123	4321	129.78.3.10	16542
10.200.60.123	2312	129.78.3.10	8754
192.168.17.8	*	129.78.3.12	*

Firewall Features

- Outbound network usage control across a boundary
- Limit inbound traffic across a boundary to a trusted network or host
- Perform NAT functions

Firewall Policy

- Security Policy Enforcement
  - Rules should justifiable with respect to security policy, guidelines, standards or practices
  - Access control list entry parameters consist of
    - Source port, source ip address, destination port, destination ip address
    - Rule order typically matters
      - First rule to match traffic in question will be applied

NAT Policy

- Configure internal host range that will be mapped and to what IP addresses
- Static NAT needs to be configured
  - Useful for providing access to system residing in a secured network and possibly lacks a routable address.

Pfsense Firewall Administration

- Console
  - – Minimal configuration
  - – Operational control
- Trusted client
  - – Web based policy administration

VMWare Networking

- Limited to Layer 2 (NICs and switches)
- All other networking services are provided by VMs you configure and manage
  - Firewalls
  - Routing
  - NAT