Mobile Access Server-
Reverse Proxy

Robert Kite, Ph.D.
SARCOM
Robert.Kite@sarcom.com

James Lovingood
SARCOM
James.Lovingood@sarcom.com

Security Overview

Balancing Security & Mobility

Security

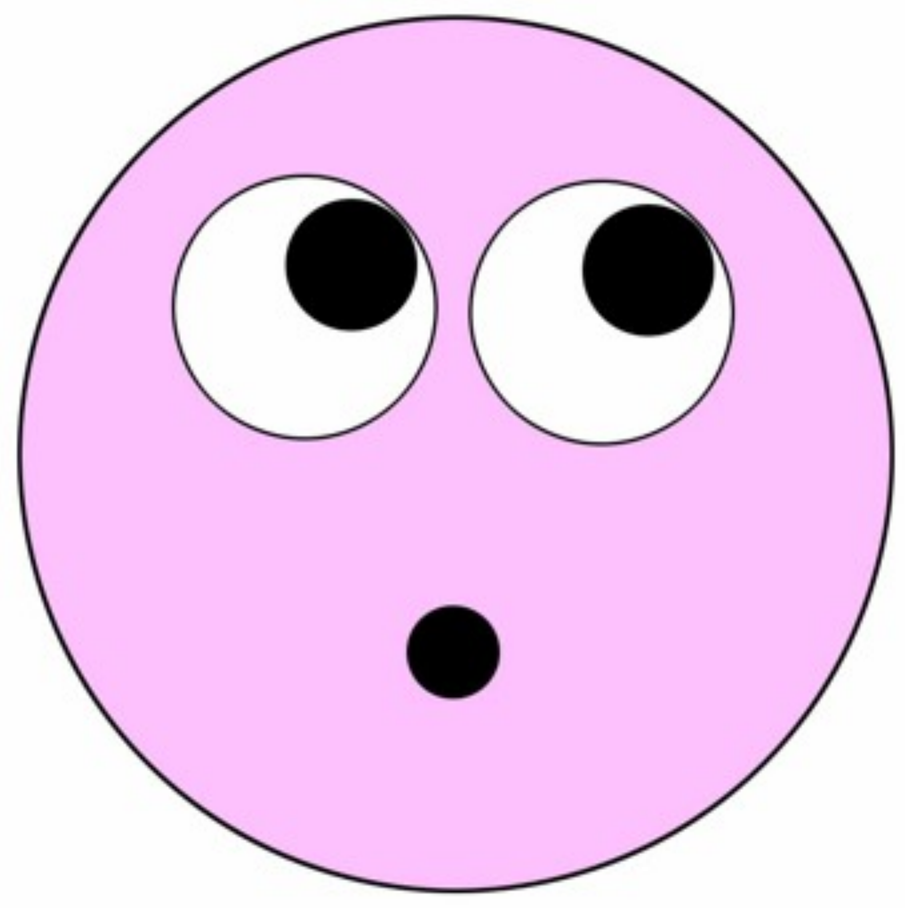
- **Prevent downtime**
- **Contain costs**
- **Reduce liability**
- **Protect sensitive info**

Mobility

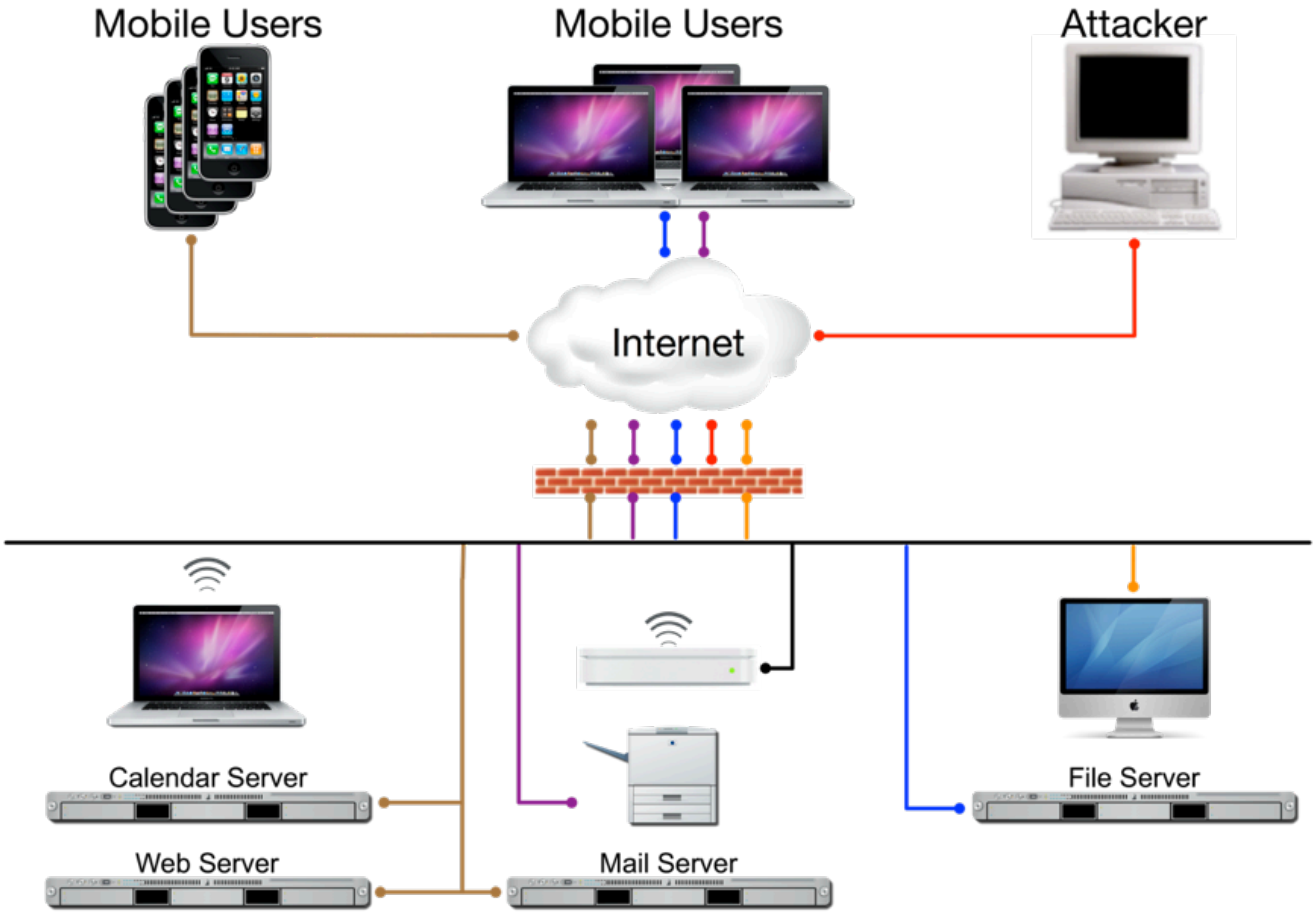
- Users access LAN from WAN
- Users work in social context
- Minimum complexity

Security Considerations

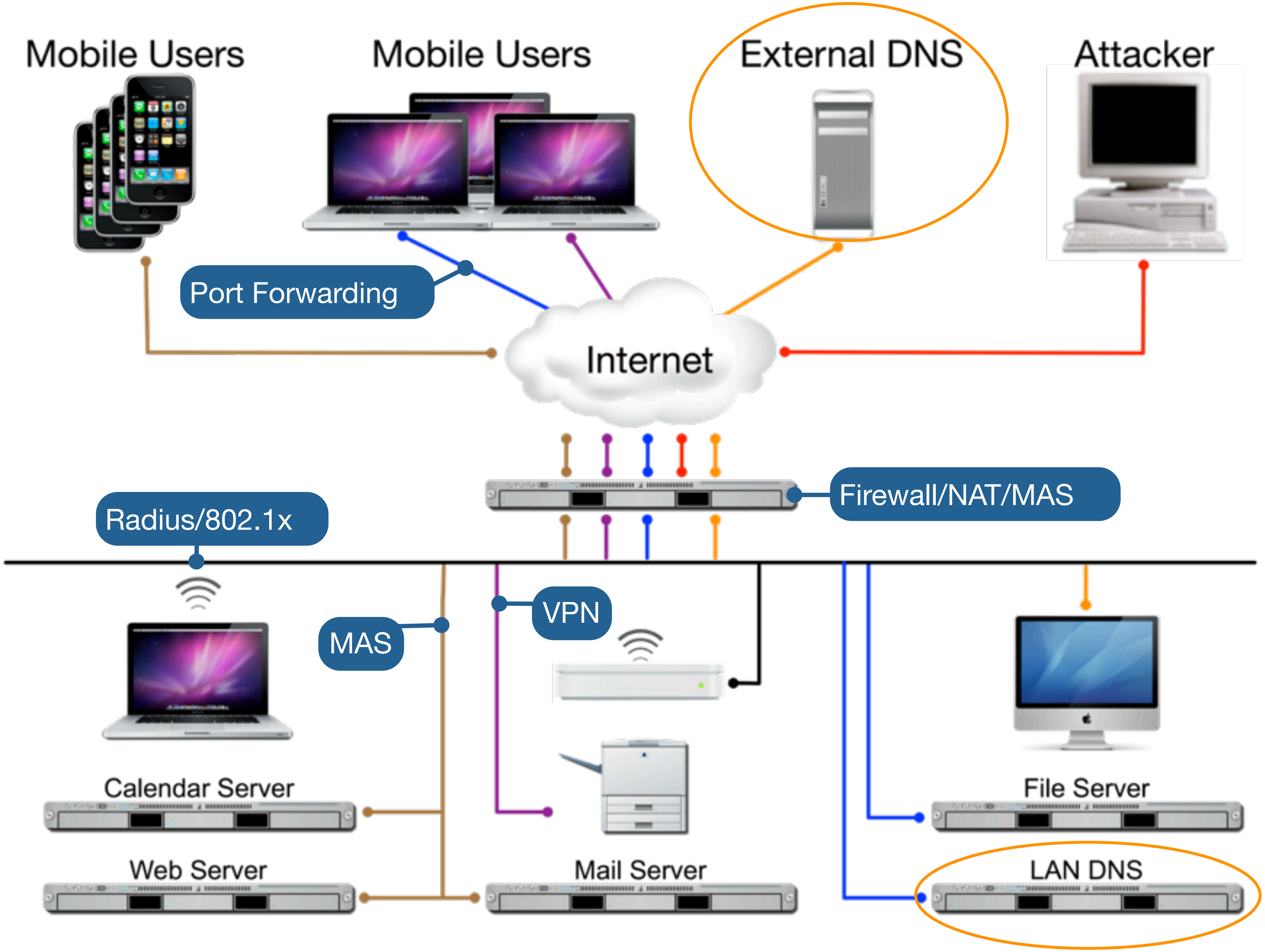
- Most services on a network are provided by having a daemon listening on a particular network port
- All packets that go past an attacker can be read by the attacker
- If an attacker has control over some part of the routing, packets can be replaced with alternate packets



Problem...

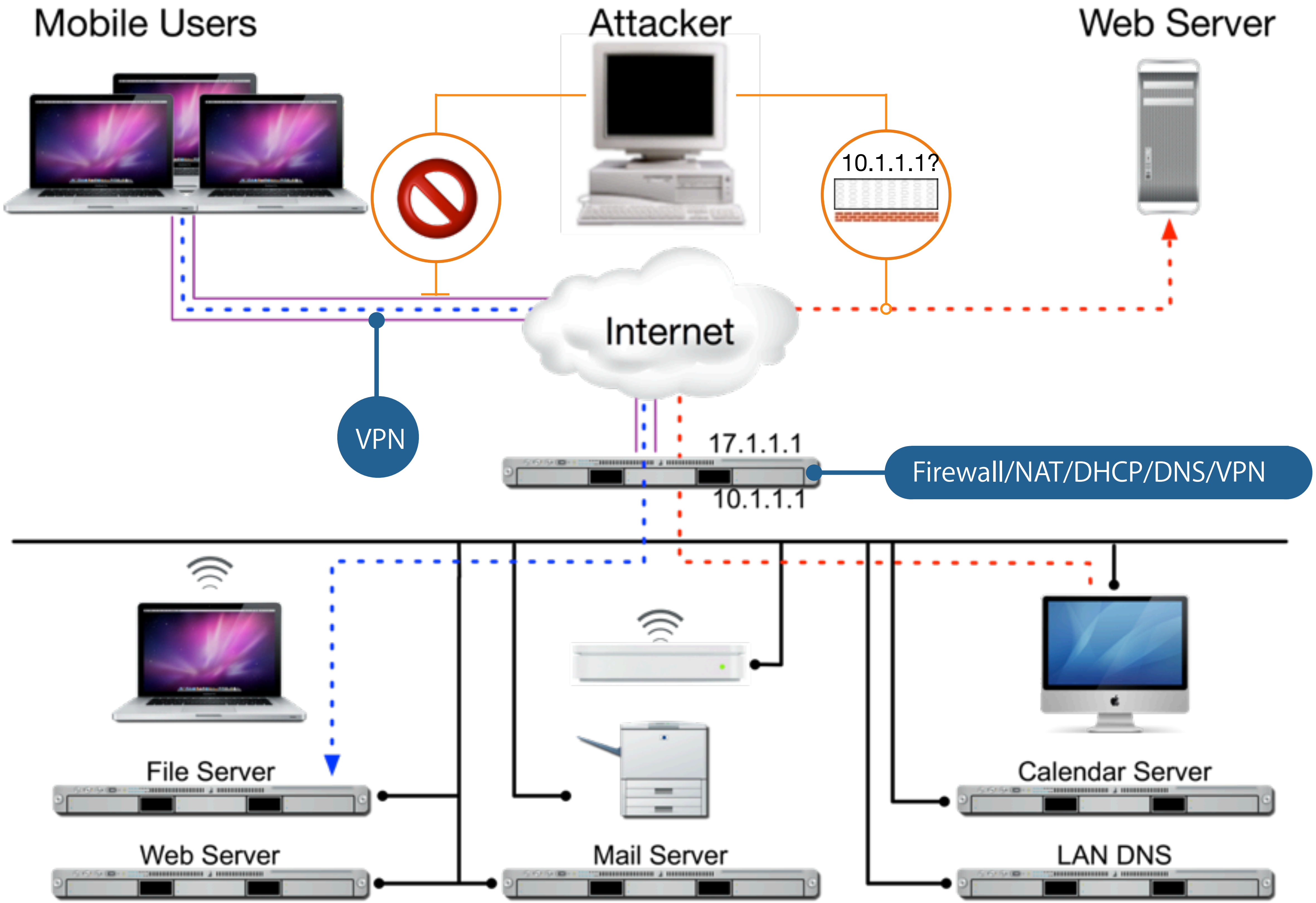

Mobile Users
Mobile Users
Attacker
Internet
Calendar Server
Web Server
Mail Server
File Server

Solutions...


Mobile Users
Mobile Users
External DNS
Attacker
Port Forwarding
Internet
Firewall/NAT/MAS
Radius/802.1x
VPN
MAS
Calendar Server
Web Server
Mail Server
File Server
LAN DNS

Gateway Setup Assistant

Gateway Setup Assistant



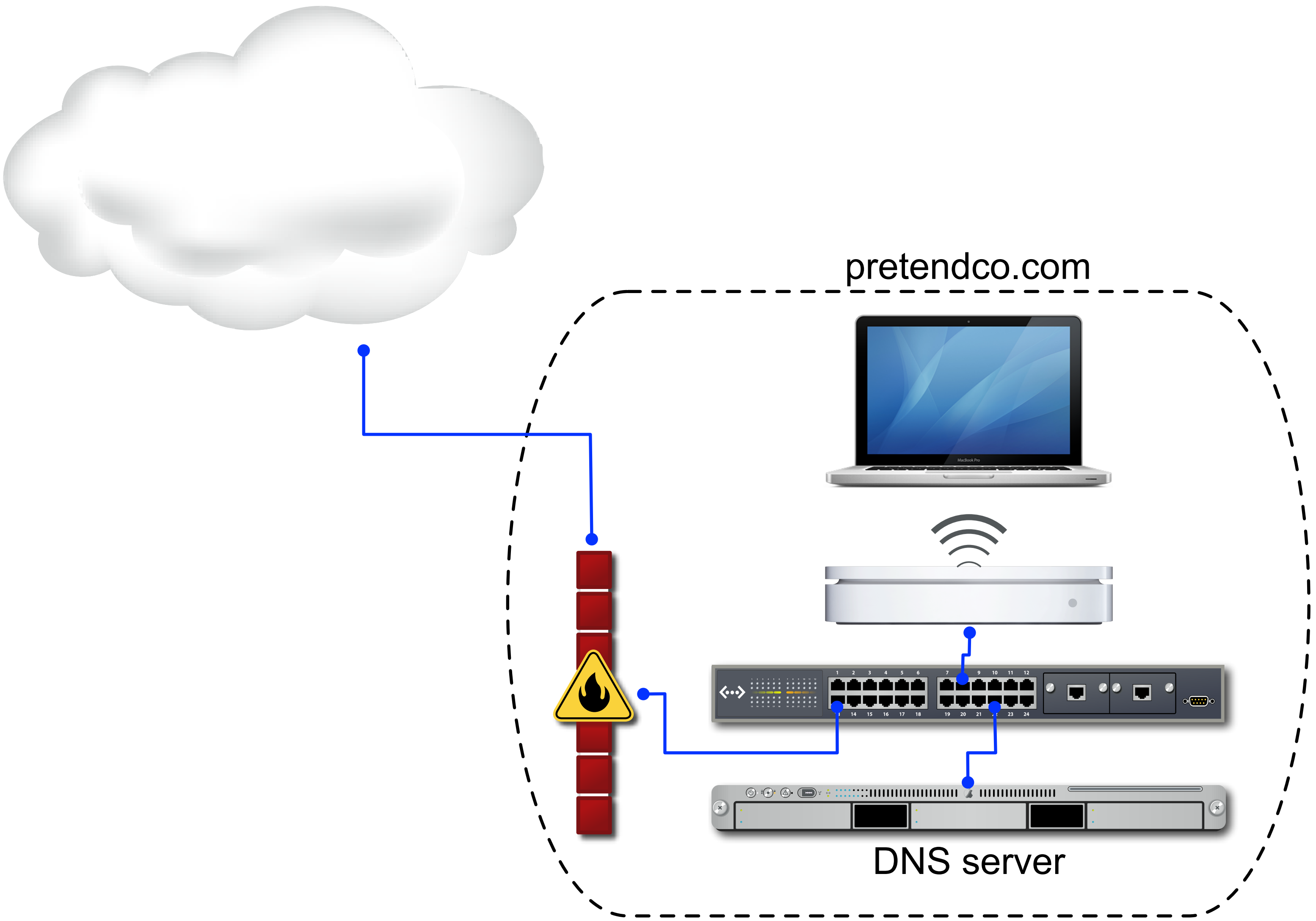
Gateway Setup Assistant

Conveniently configures…

- DHCP (192.168.x.1 subnet only)
- DNS (Caching DNS only)
- Firewall (very basic configuration)
- NAT
- VPN (optional)

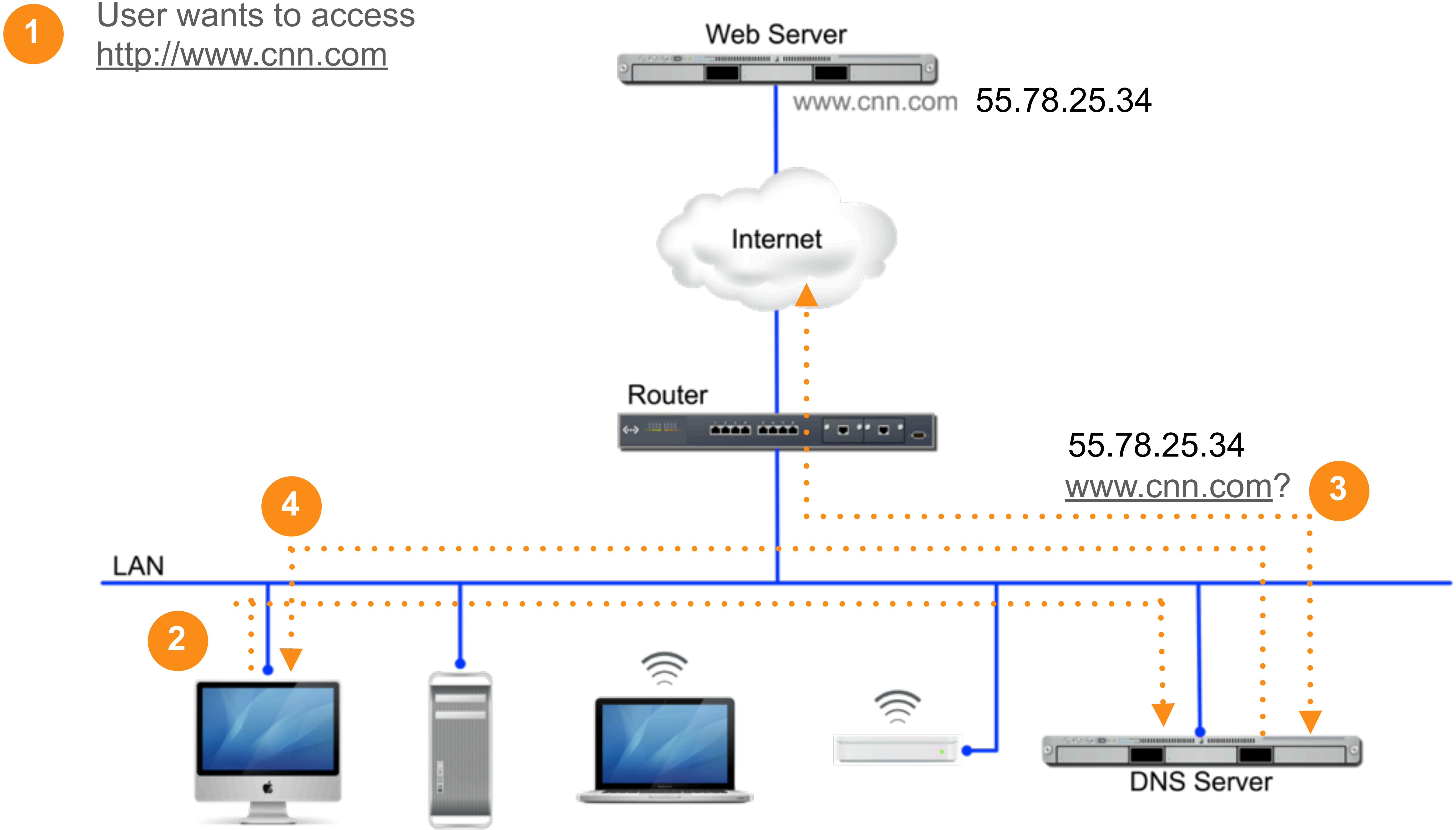
DNS

DNS Basics

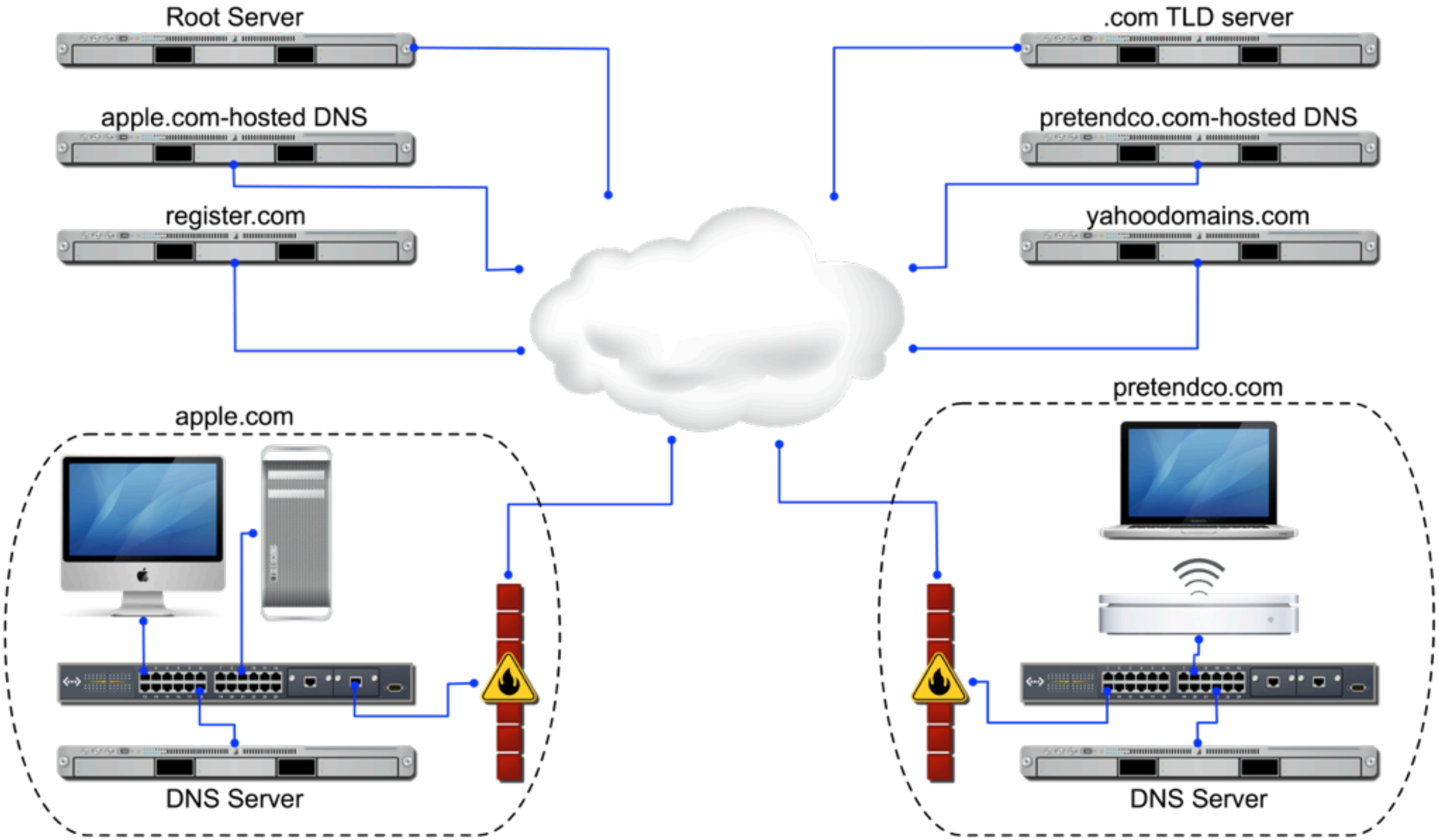


Domain Name System (DNS)

1 User wants to access
http://www.cnn.com



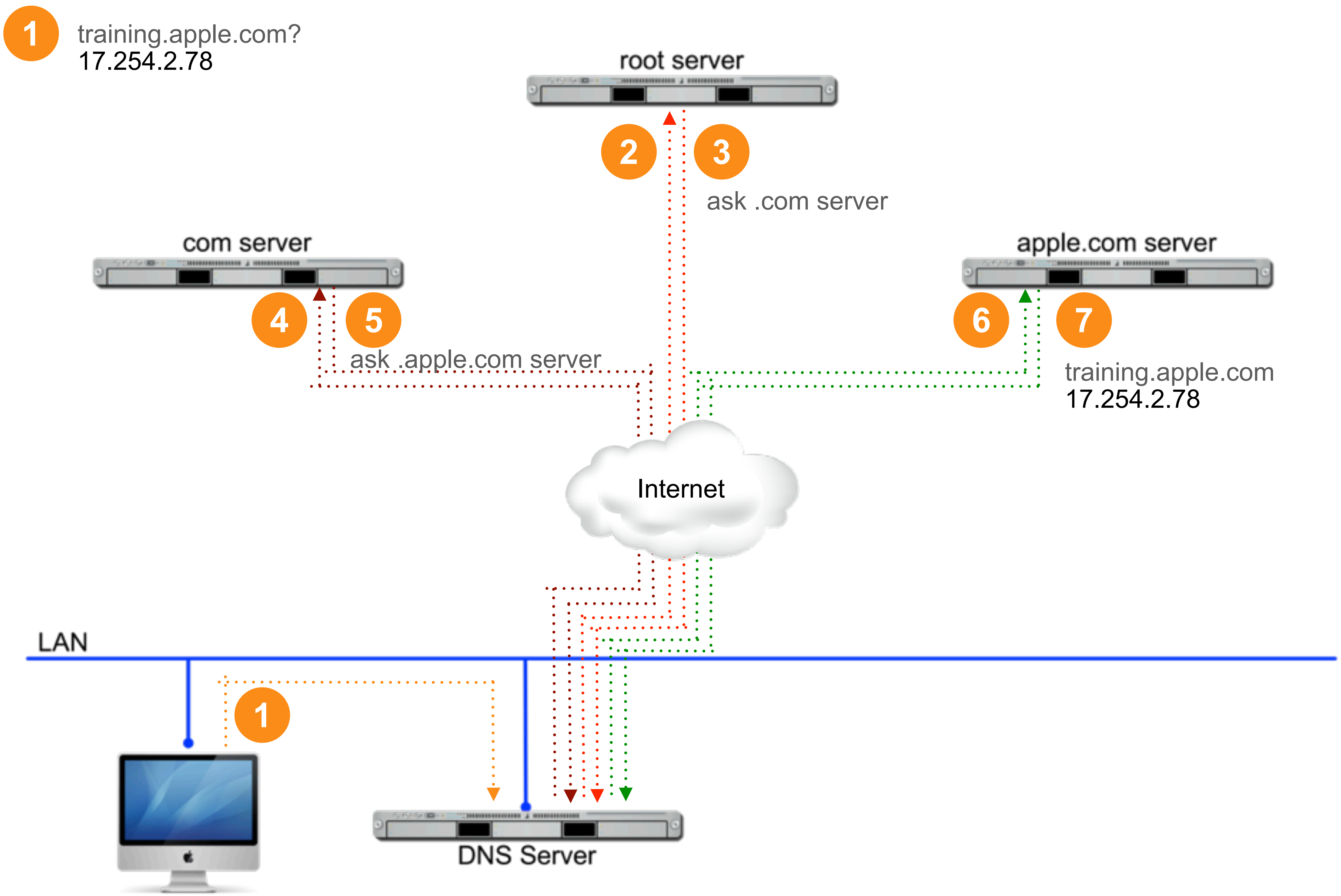
DNS Query Path



DNS: The Big Picture

- Converts IP addresses to easy to remember names
- Can be provided by ISP or hosted internally
- Public domain names must be registered
- Uses recursive queries to locate and resolve remote machine names on other networks
- Required for several network and authentication services
  - Kerberos
  - Directory Services (including Open Directory & Active Directory)
  - Mail

DNS Basics



1 training.apple.com?
17.254.2.78

root server

2

3

ask .com server

com server

4

5

ask .apple.com server

apple.com server

6

7

training.apple.com
17.254.2.78

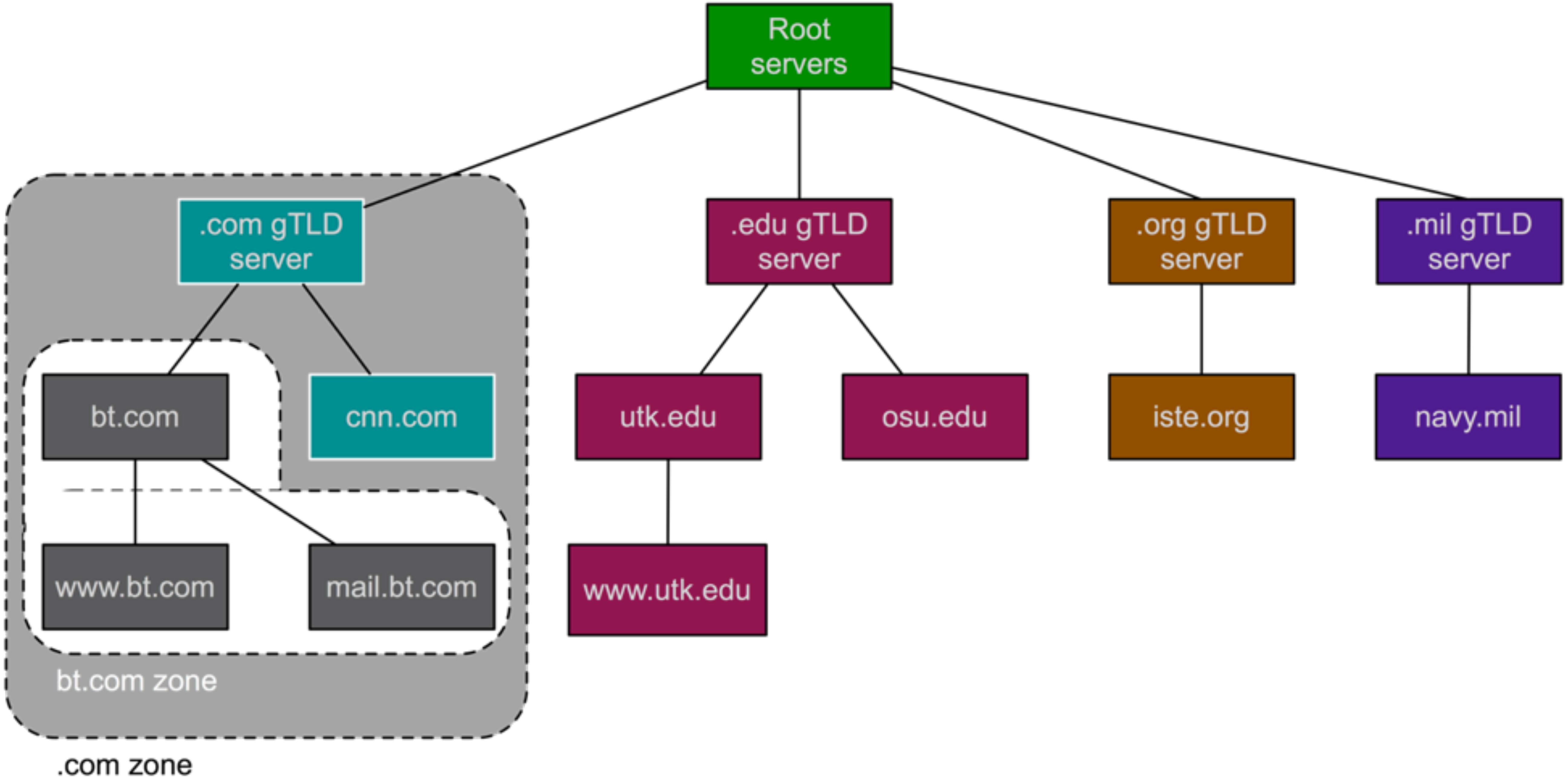
Internet

LAN

1

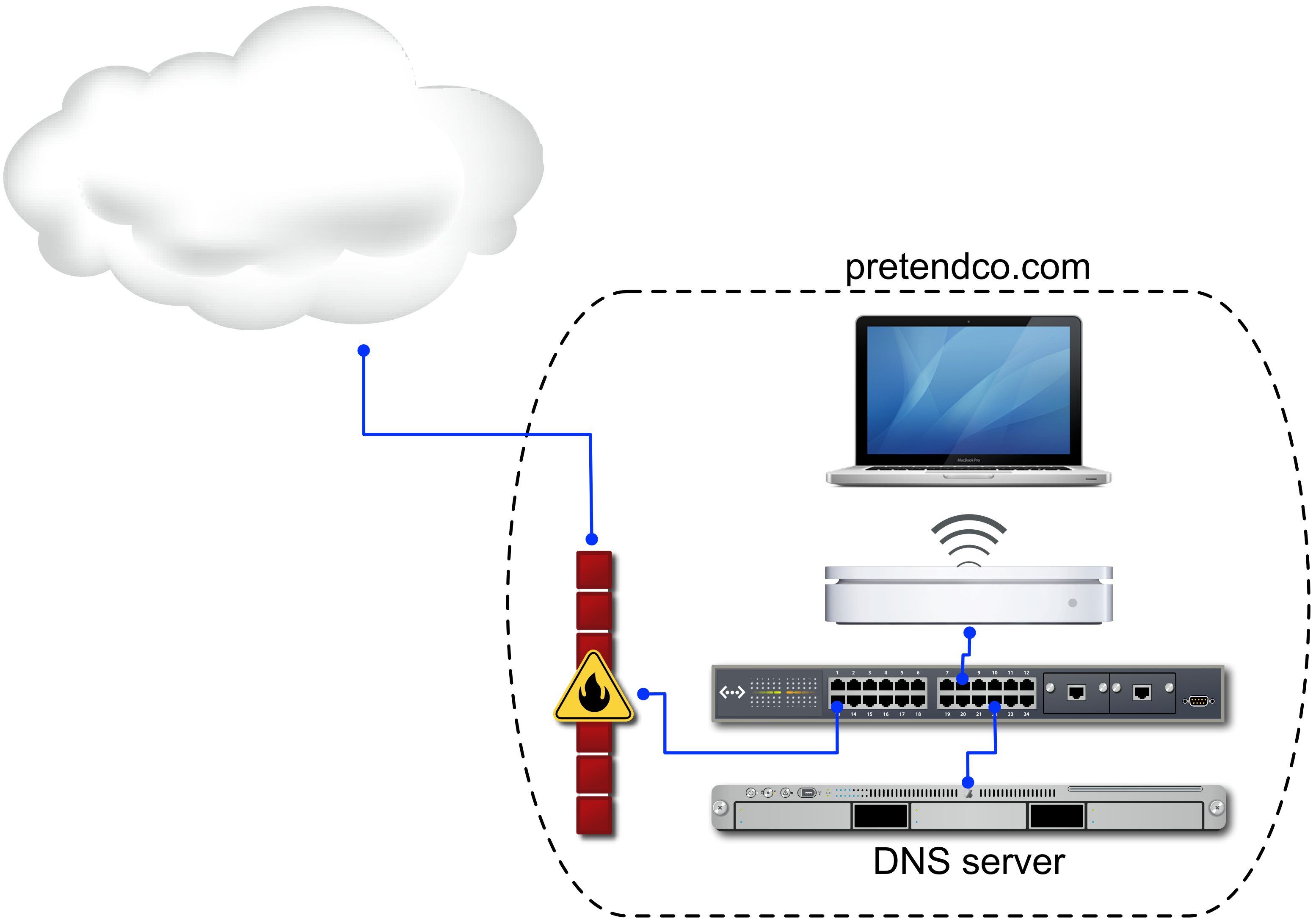
DNS Server

Domains, Zones, Computers



DNS Security

5 Types of Attacks



DNS Server Mining

Obtain copy of complete zone

- Hackers request zone transfer of primary zone.
- Determine what services a domain offers and the servers providing those services
- Try specific attacks against those services
- Prevention - disable zone transfers or only allows specific IPs to request a transfer

Zone Transfer Security

Verify whether your zone allows transfers

- If allowed, anyone can request a copy of the entire zone

Two different approaches to secure zone transfers

- Firewall
  - Block TCP port 53 to all except secondary DNS servers
- Configure named
  - `allow-transfer {10.1.1.1; 10.1.17.1 };`
  - Required to maintain the zone outside of Server Admin

DNS Service Profiling

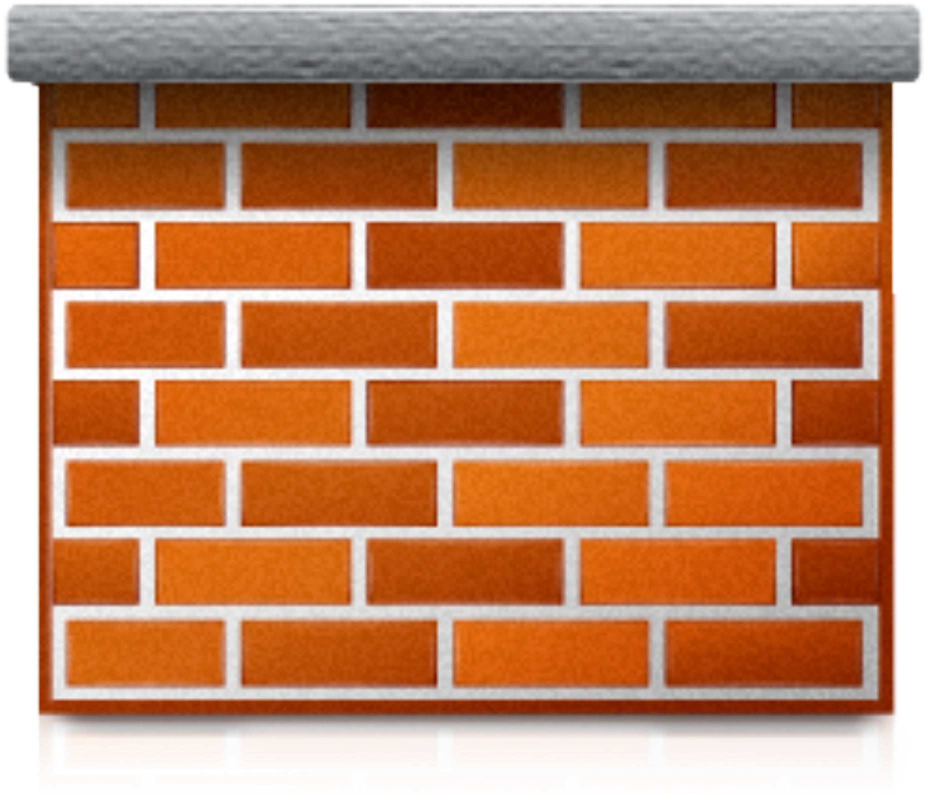
Bind version request

- Hackers request the version of BIND running on a server
- Compare the version number to known exploits and vulnerabilities
- Prevention - configure BIND to respond with something other than what it is.
- `version “None of your business!”;`

DNS Denial of Service

Overloading DNS Server

- Hackers send more requests than server or network can handle
- Prevention
  - Constantly monitor DNS service and server load.
  - Block the offending IP address with a firewall.

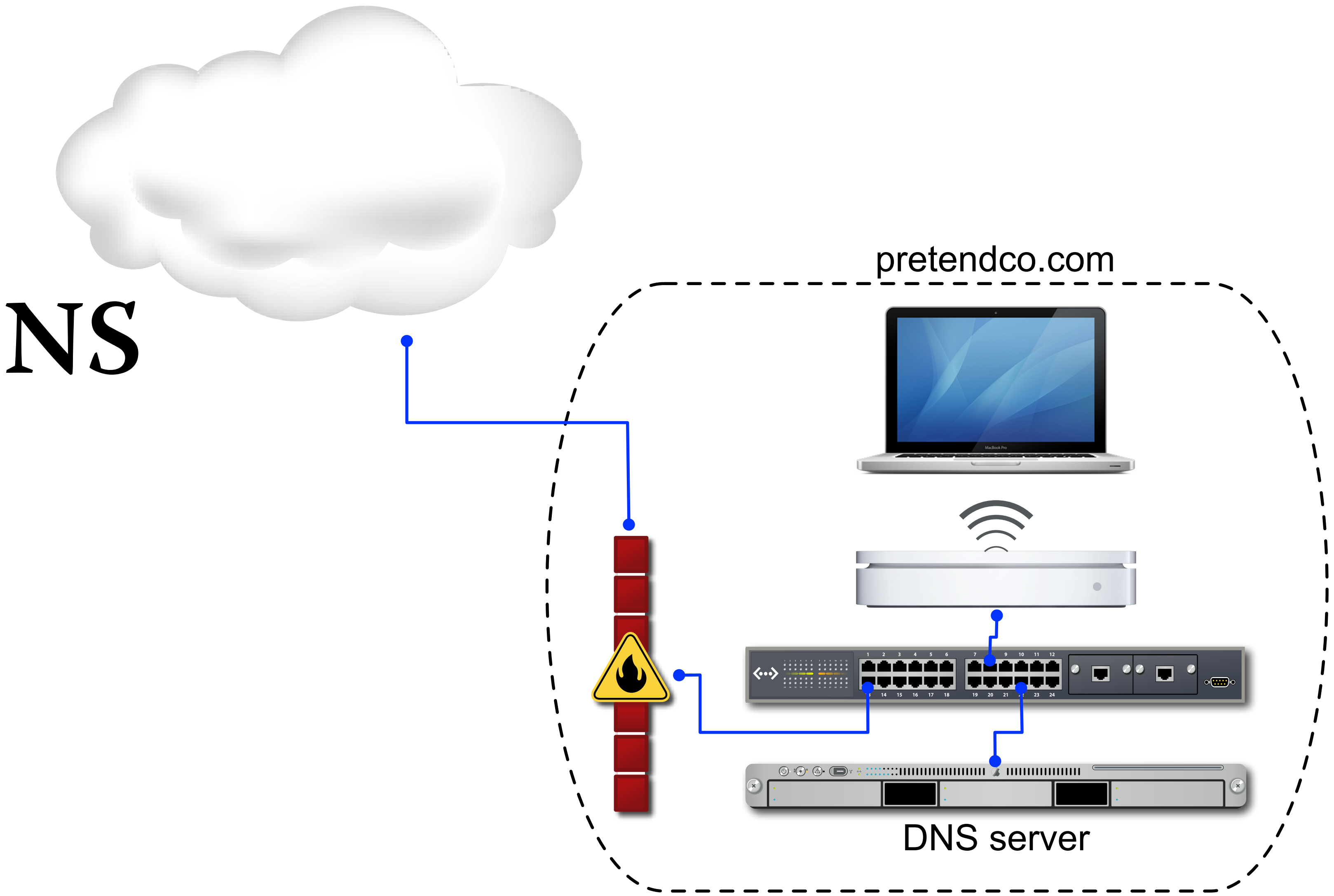


DNS Service Piggybacking

Not using your own DNS

- Not using the DNS server provided by ISP or administrator
- Results in DNS server being accessed by more users than planned
- Prevention
  - Limit or disable recursion

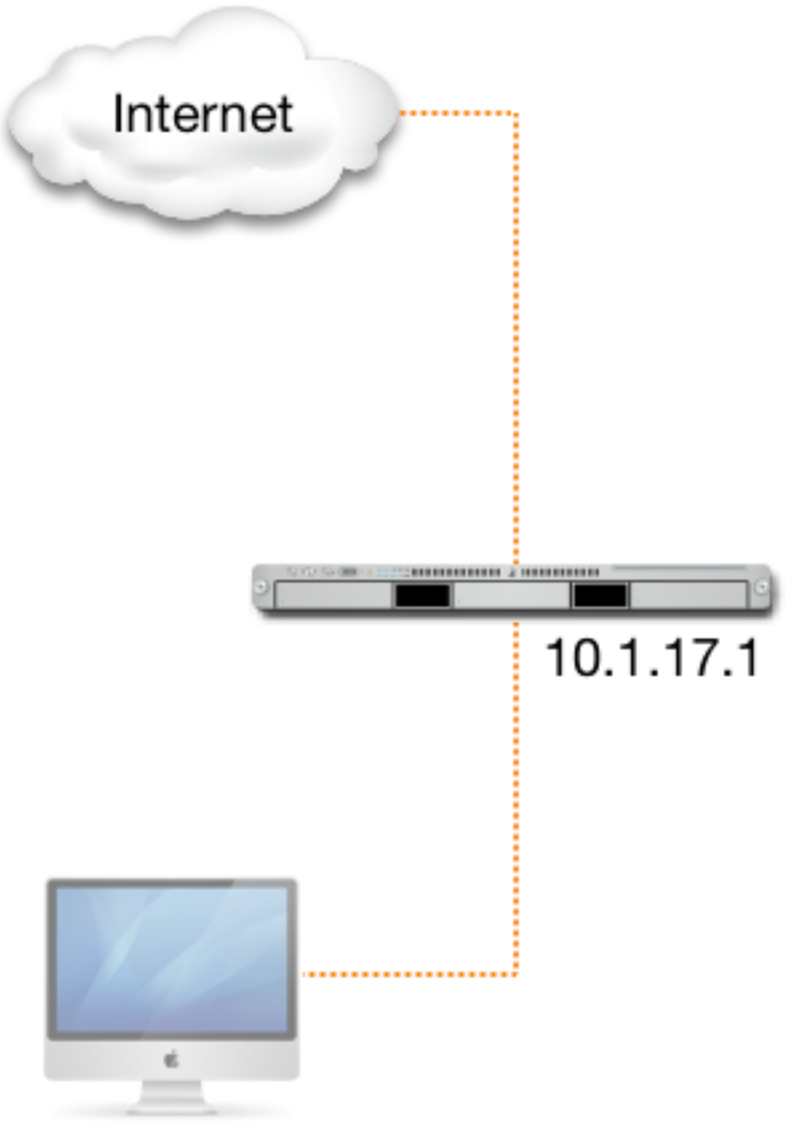
Secure & Private DNS

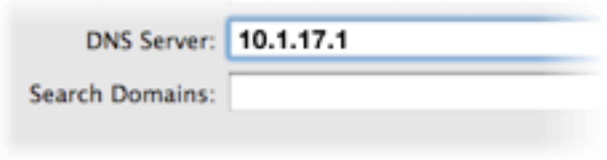


Caching-Only

DNS Server for caching DNS queries

- Inside the firewall and local to the network
  - Saves trips to the Internet
  - Faster Connection
- Still need to be secured
  - Default configuration is OK (localnets)
  - Limit to specific subnets to reduce load





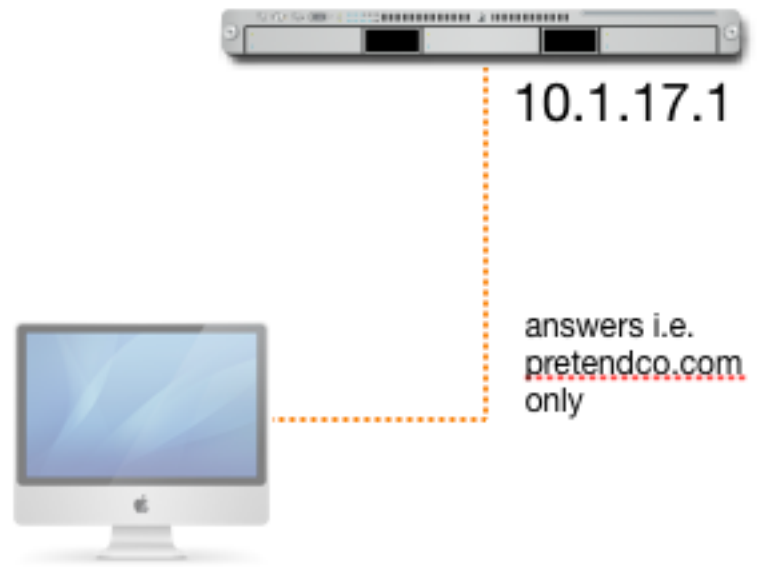
DNS Server: 10.1.17.1

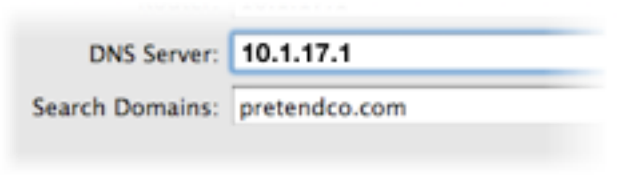
Search Domains:

Authoritative-Only

Authoritative-Only Services

- Provide answers only to their own zones
  - Primary and secondary zones
- Recursive queries not allowed

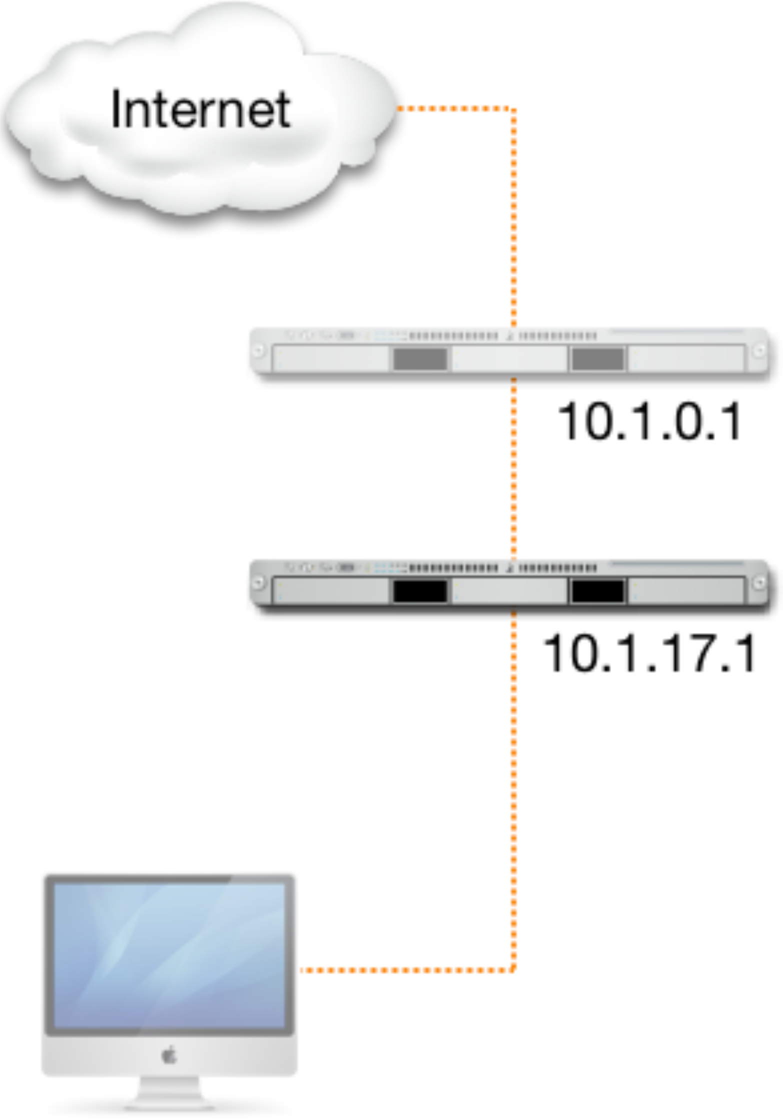


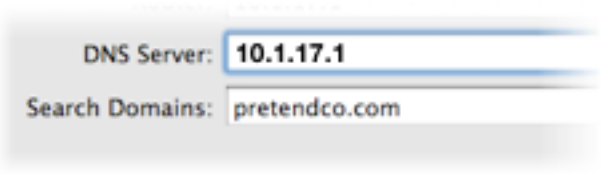

DNS Server: 10.1.17.1
Search Domains: pretendco.com

Forwarders

Similar to Authoritative-Only

- Provide answers only to their own zones
  - Primary and secondary zones
- Recursive queries are forwarded to other servers

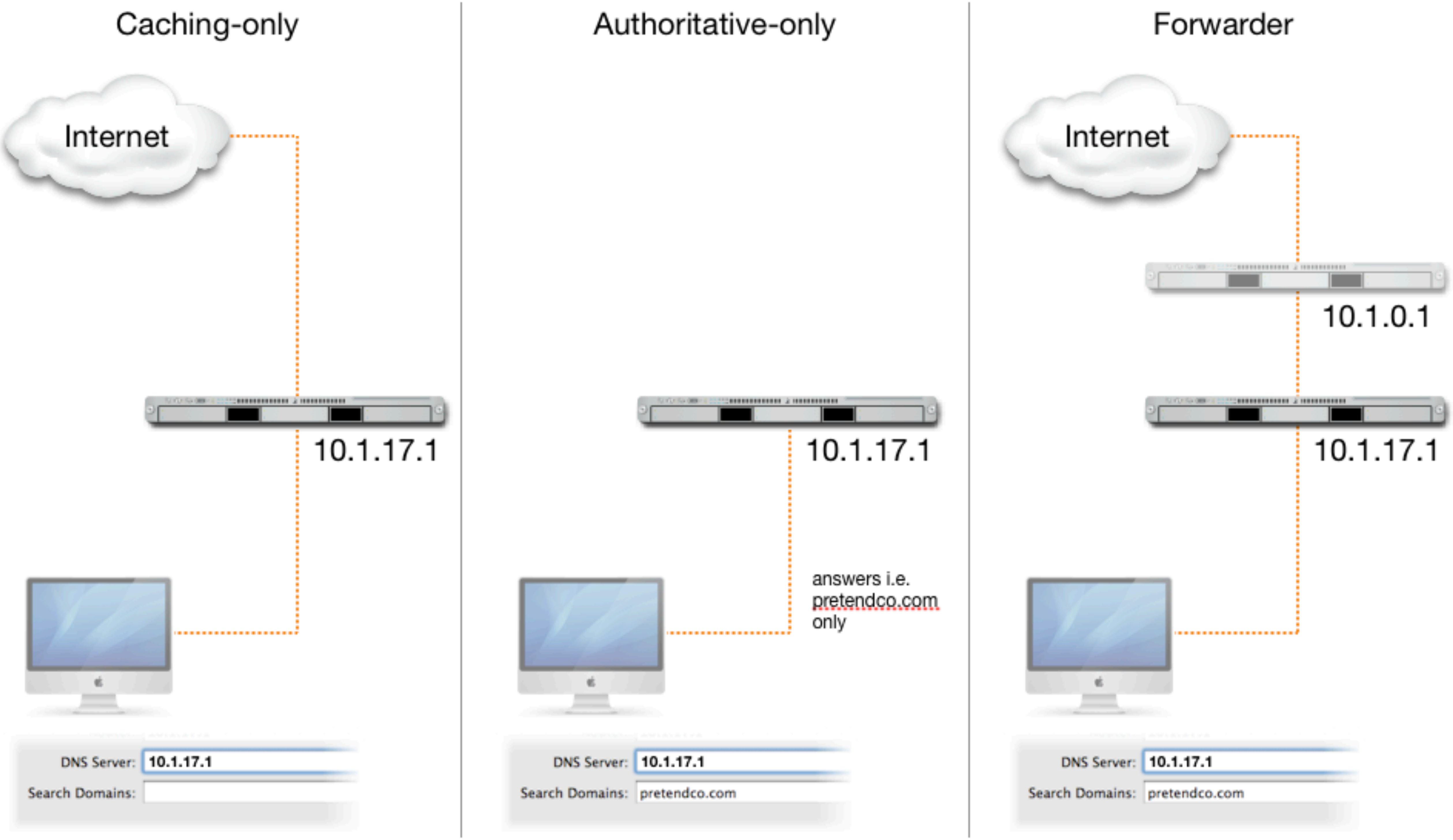




DNS Server: 10.1.17.1

Search Domains: pretendco.com

Comparison



Caching-only

DNS Server: 10.1.17.1

Search Domains:

Authoritative-only

answers i.e. pretendco.com only

DNS Server: 10.1.17.1

Search Domains: pretendco.com

Forwarder

DNS Server: 10.1.17.1

Search Domains: pretendco.com

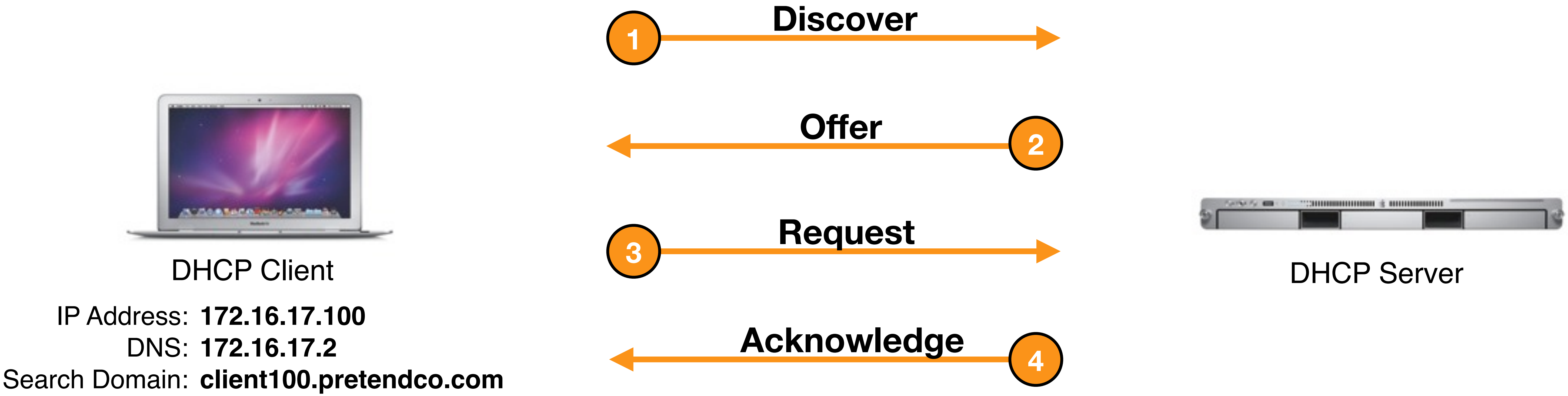
DHCP

DHCP Basics

Dynamic Host Configuration Protocol

- Assigns clients unique IP address
- Uses a range of IP addresses
  - Each range referred to as a subnet
  - Static mapping IP addresses
- Can provide additional network configuration
  - Default router, DNS and search domain, LDAP, WINS

How DHCP Works (DORA)



1 Discover

2 Offer

3 Request

4 Acknowledge

DHCP Client

IP Address: **172.16.17.100**
DNS: **172.16.17.2**
Search Domain: **client100.pretendco.com**

DHCP Server

Security Considerations

Avoid using DHCP whenever possible!

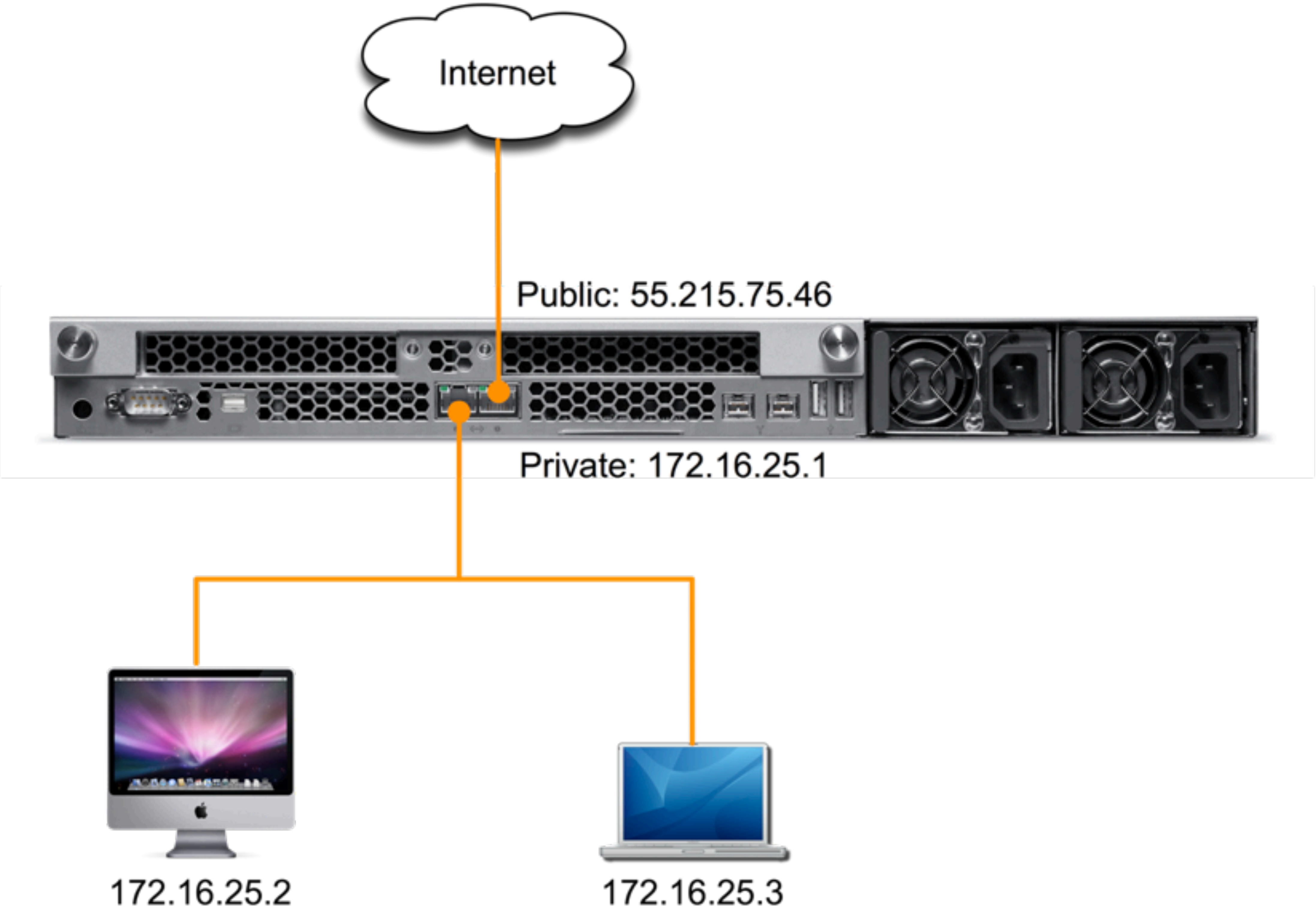
- Eases accountability and mitigates the risks posed by rogue DHCP servers
  - Invalid IP addresses could be distributed

If you MUST use DHCP

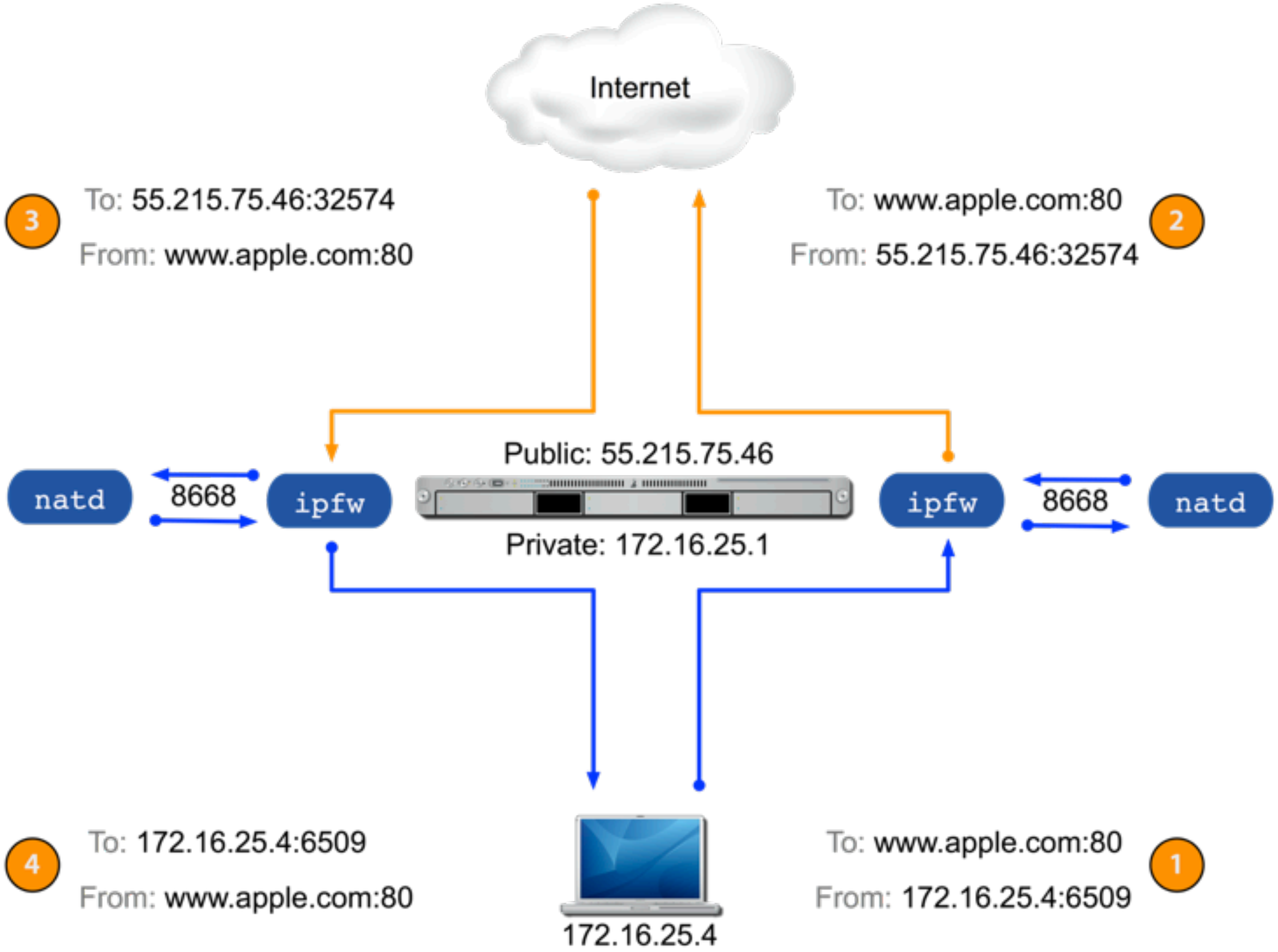
- Static Mapping
- Do not distribute DNS, LDAP, or WINS information
  - Option 95 (LDAP) not supported in Mac OS X 10.6
  - Users could be assigned incorrect DNS servers and directed to malicious websites or servers.

NAT

Network Address Translation (NAT)



How NAT Works



[illegible] requester

then forwards back to firewall. Firewall delivers request as if coming from itself.

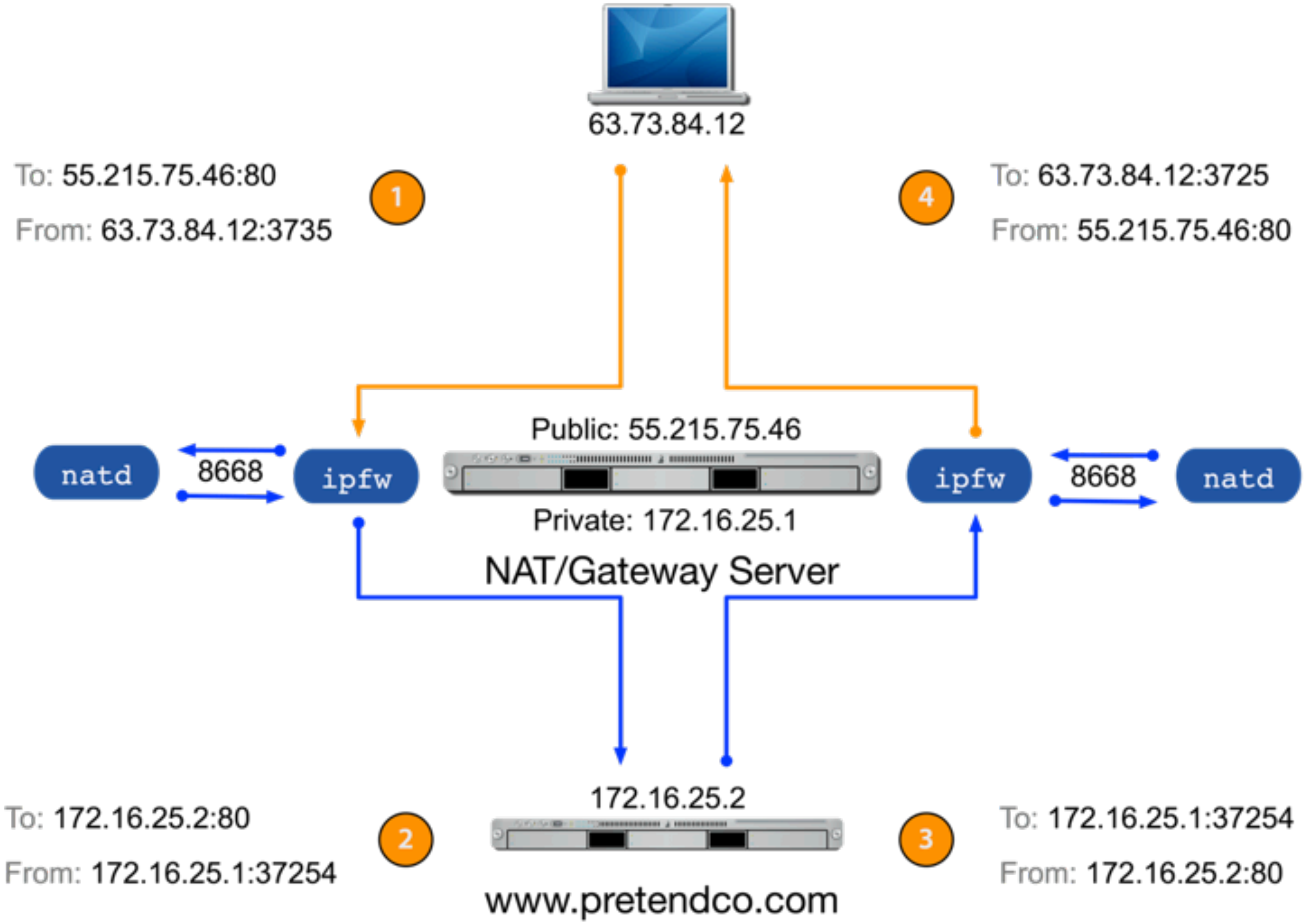
processes and forwards back to firewall.

Firewall

Packet Divert Rule

- Rule is added to firewall when NAT service is enabled
- Diverts all incoming and outgoing traffic to natd for processing
- Firewall service must be started for any firewall rule to an effect
- Communicates with natd over port 8668

How Port Forwarding Works



[illegible] the
[illegible] and port number.

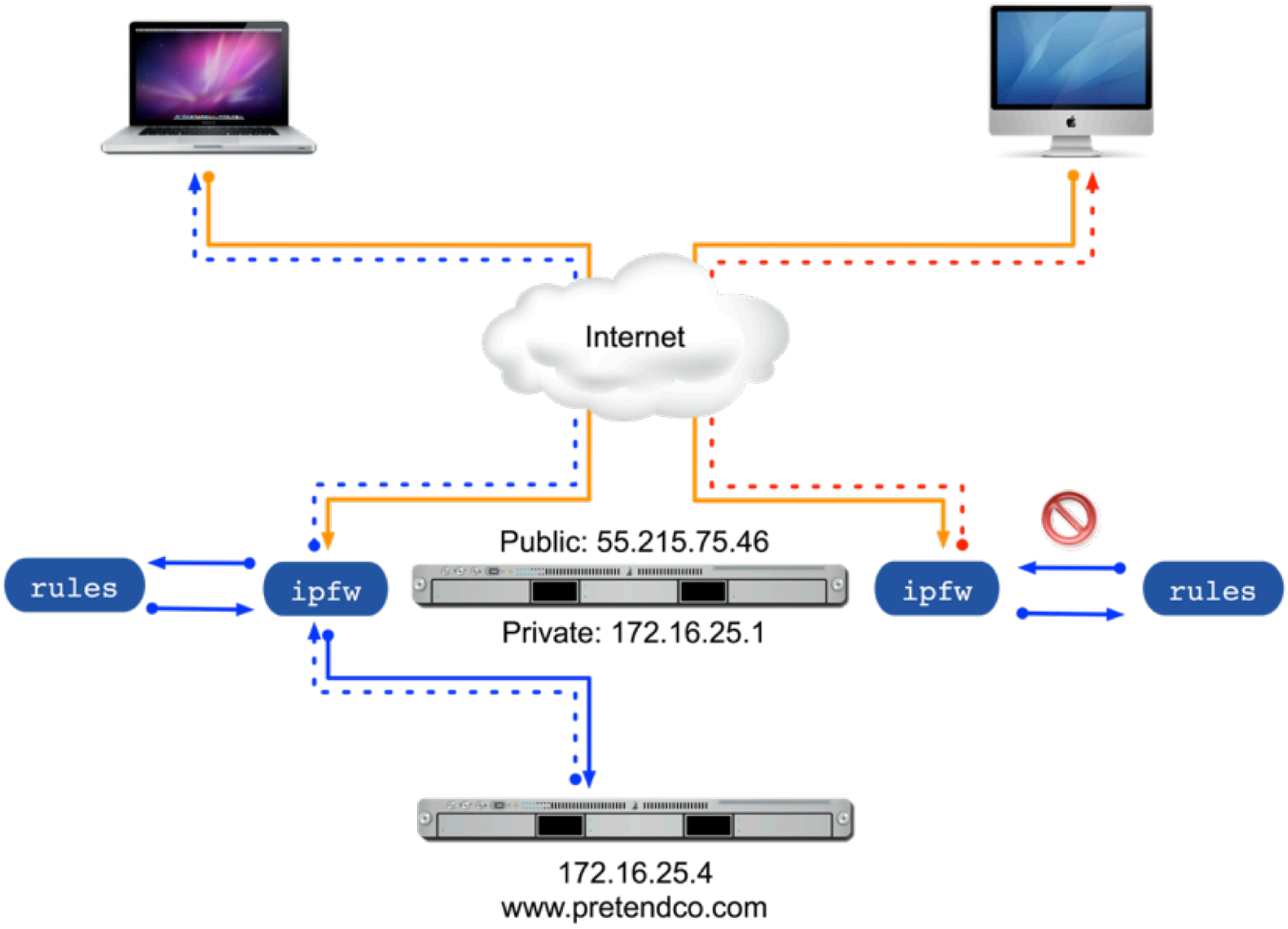
Security Considerations

The NAT service, by design, offers a layer of security between you private LAN and public network:

- External computers cannot determine a private IP address. This creates a barrier between your private network and the public network
- Communication from a public network cannot come into your private network unless it is requested or port forwarding has been configured
- Allowing clients to automatically configure PAT (UPnP) may not be a good idea
- Port Forwarding does not allow you to control who accesses your services

Firewall

How Firewall Works



Firewall Rules

Format:

- `action protocol from source to destination interface-spec options`

Control traffic by:

- Network protocol type
- Source IP address and port
- Destination IP address and port
- Inbound/outbound
- Interface

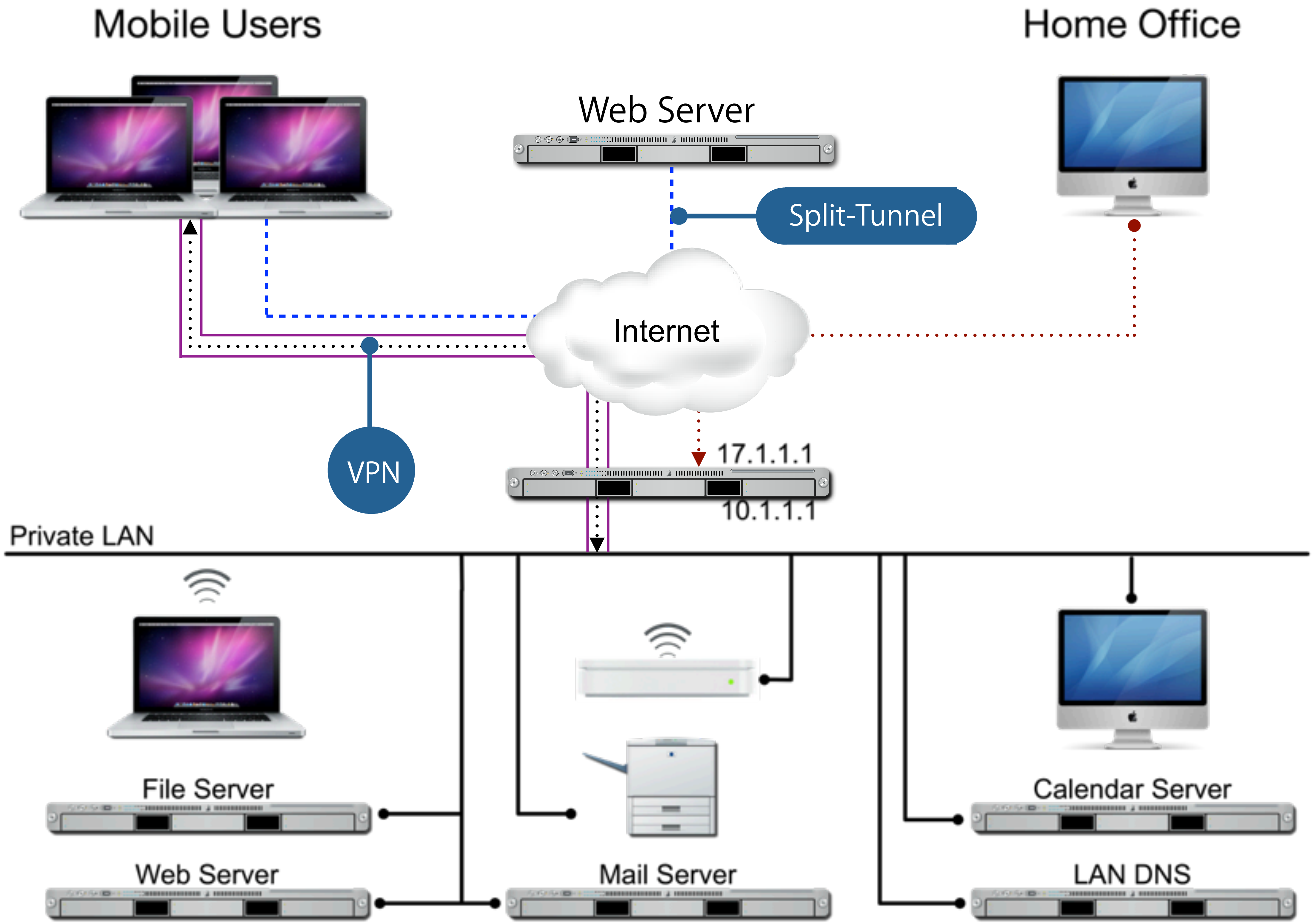
Security Considerations

Firewall

- Only open required ports
- Limit open ports to specified subnets when possible
- Monitor the firewall logs

VPN

How VPN Works



L2TP vs PPTP

L2TP - Layer Two Tunneling Protocol

- Considered more secure than PPTP
- Requires specific NAT/Firewall configuration
- Supports machine-based certificates

PPTP - Point-to-Point Tunneling Protocol

- Easier to configure
- Lower overhead
- Considered less secure than L2TP

Protocol and Security Support

Client-Side Protocol Options

	L2TP	PPTP	Cisco IPSec
OS X Clients	✔	✔	✔
iPhone	✔	✔	✔

VPN Authentication Options

	L2TP	PPTP	Cisco IPSec
OD/AD	✔	✔	✔
Secret	✔		✔
Certificate	✔		
RADIUS	✔	✔	✔

Security Considerations

Server Side

- Only deploy necessary protocols
- Leverage certificates or two-factor authentication
- Use 4-bit option for PPTP sparingly

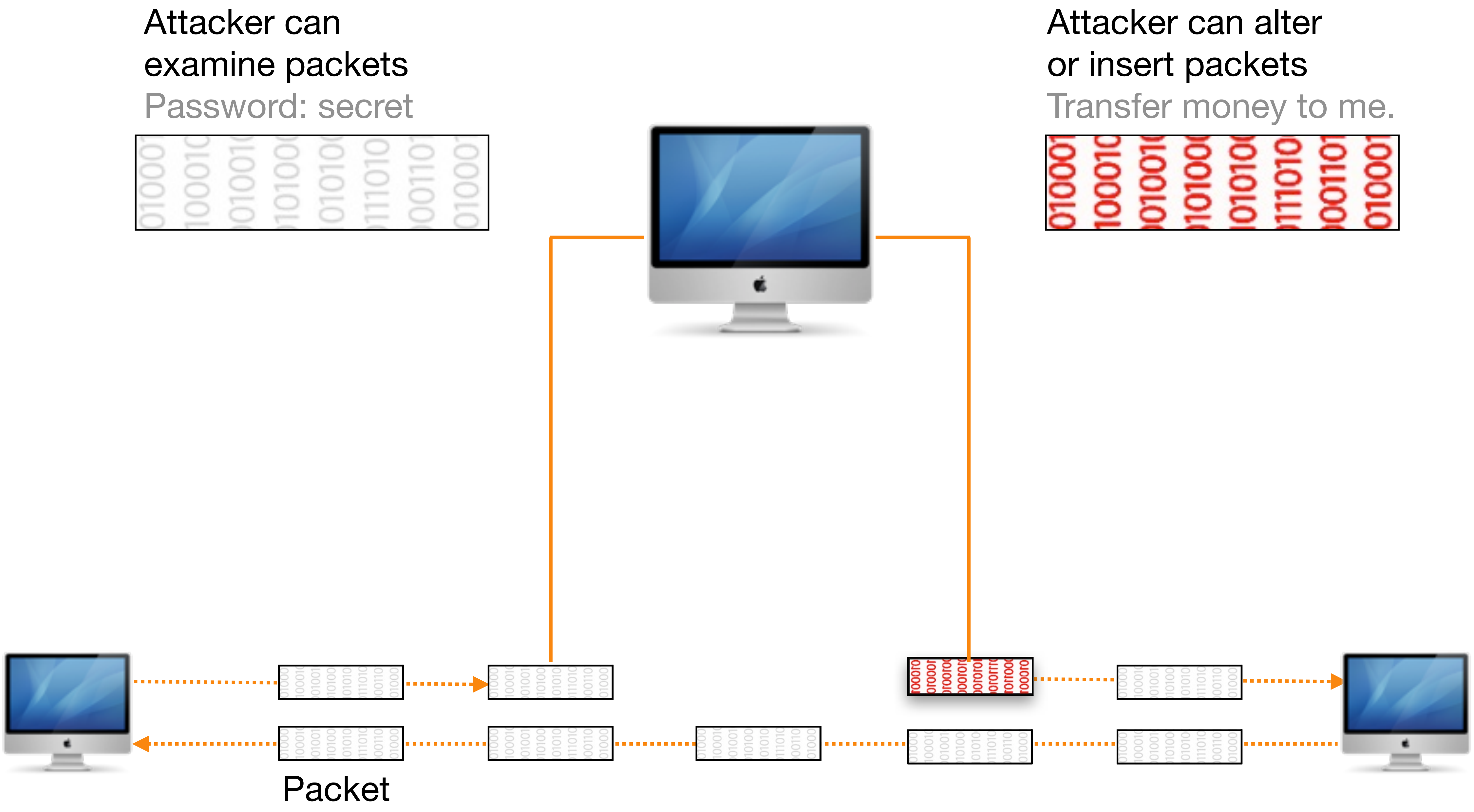
Client Side

- Split-Tunnel or no Split-Tunnel?
- Client Firewall enabled to prevent hackers

CERTIFICATES

Encryption Basics

Why Encrypt



Attacker can examine packets

Password: secret

Attacker can alter or insert packets

Transfer money to me.

Packet

Encryption

Basic Types

- Digests or one-way hashes
- Symmetric keys
- Asymmetric keys

Mac OS X Uses

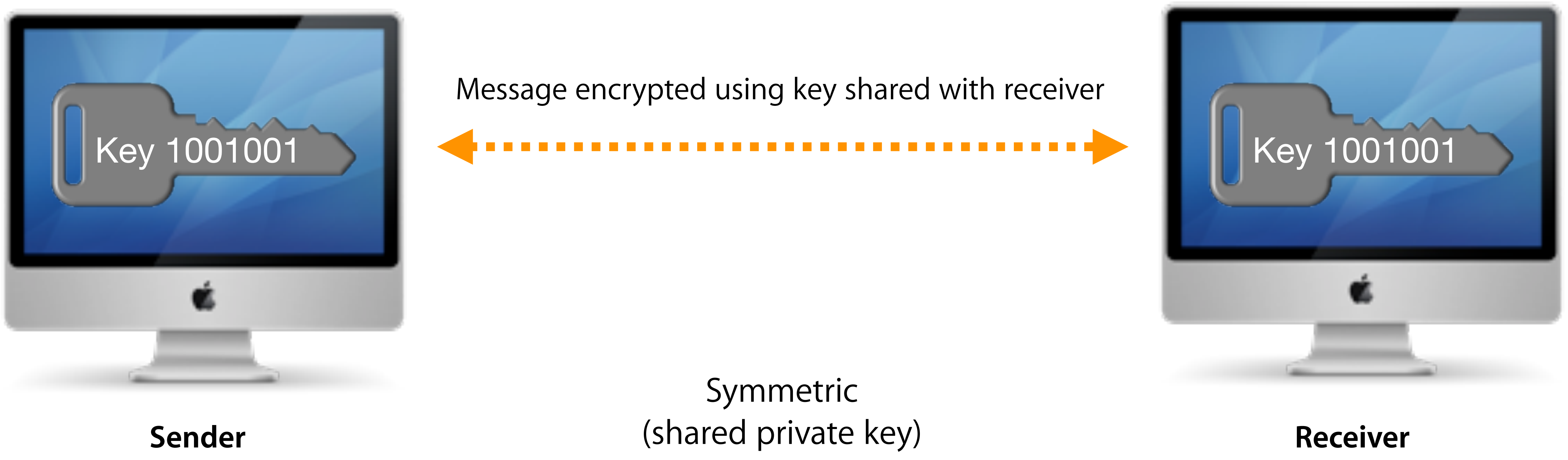
- SHA hashes are used by Apple updates
- Symmetric keys are used in Kerberos
- Asymmetric keys are used in SSL, smart cards, etc.

Digests/Hashes

A hash is also referred to as a digest or message digest

- Digital fingerprint
- One-way mathematical process
  - Secure Hash Algorithm - 1 (SHA-1, SHA-2, SHA-256)
  - Message Digest (MD-5)

Symmetric Keys - Encryption



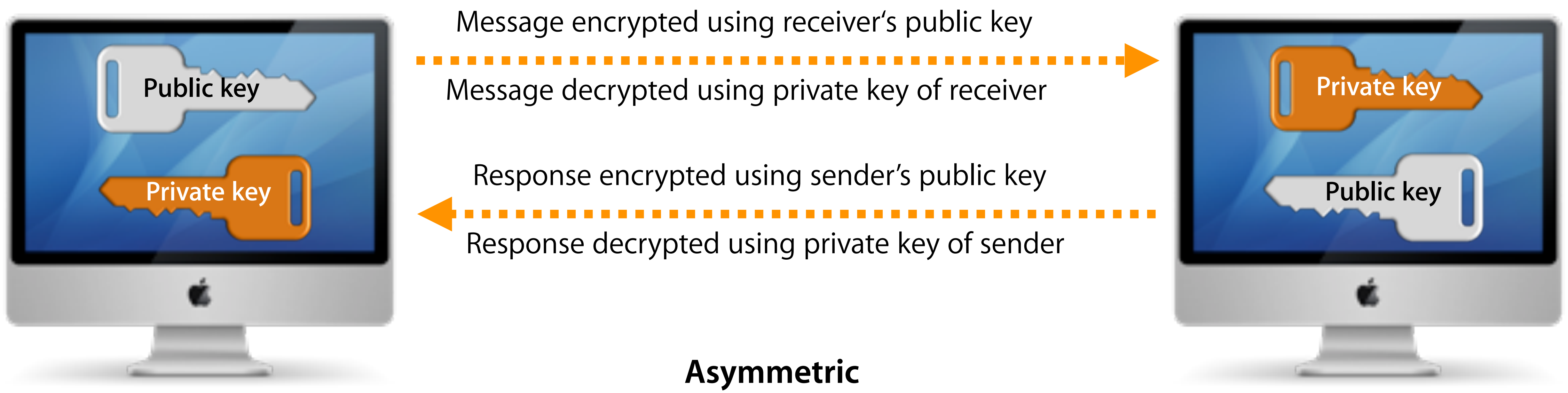
Message encrypted using key shared with receiver

Sender

Symmetric
(shared private key)

Receiver

Asymmetric Keys - Encryption



Message encrypted using receiver’s public key

Message decrypted using private key of receiver

Response encrypted using sender’s public key

Response decrypted using private key of sender

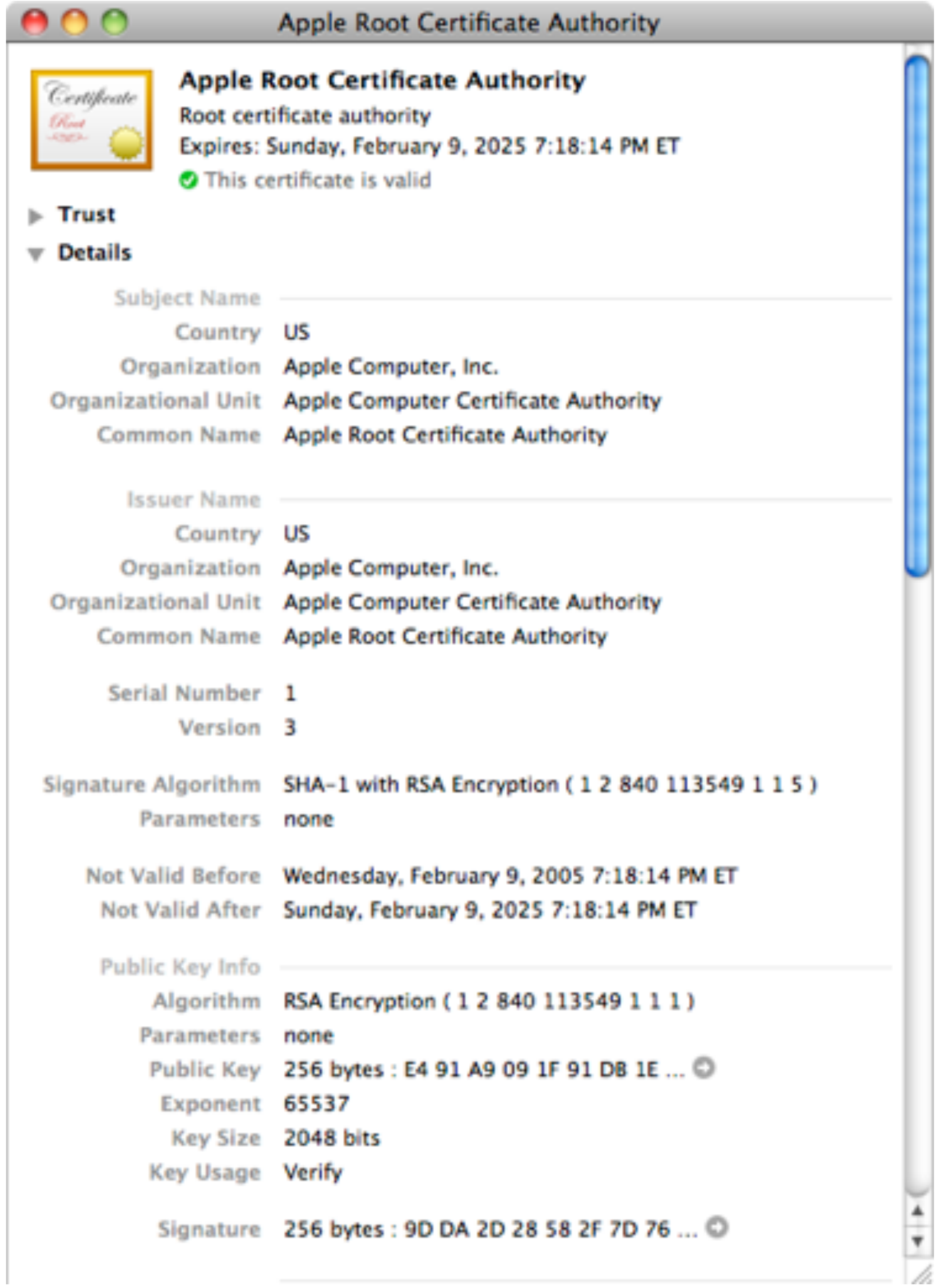
Sender

Asymmetric
(public/private key pairs)

Receiver

Certificates & Keys

Certificates contain information about the entity they are issued to and that entity's public key.



Apple Root Certificate Authority

Apple Root Certificate Authority

Root certificate authority

Expires: Sunday, February 9, 2025 7:18:14 PM ET

✓ This certificate is valid

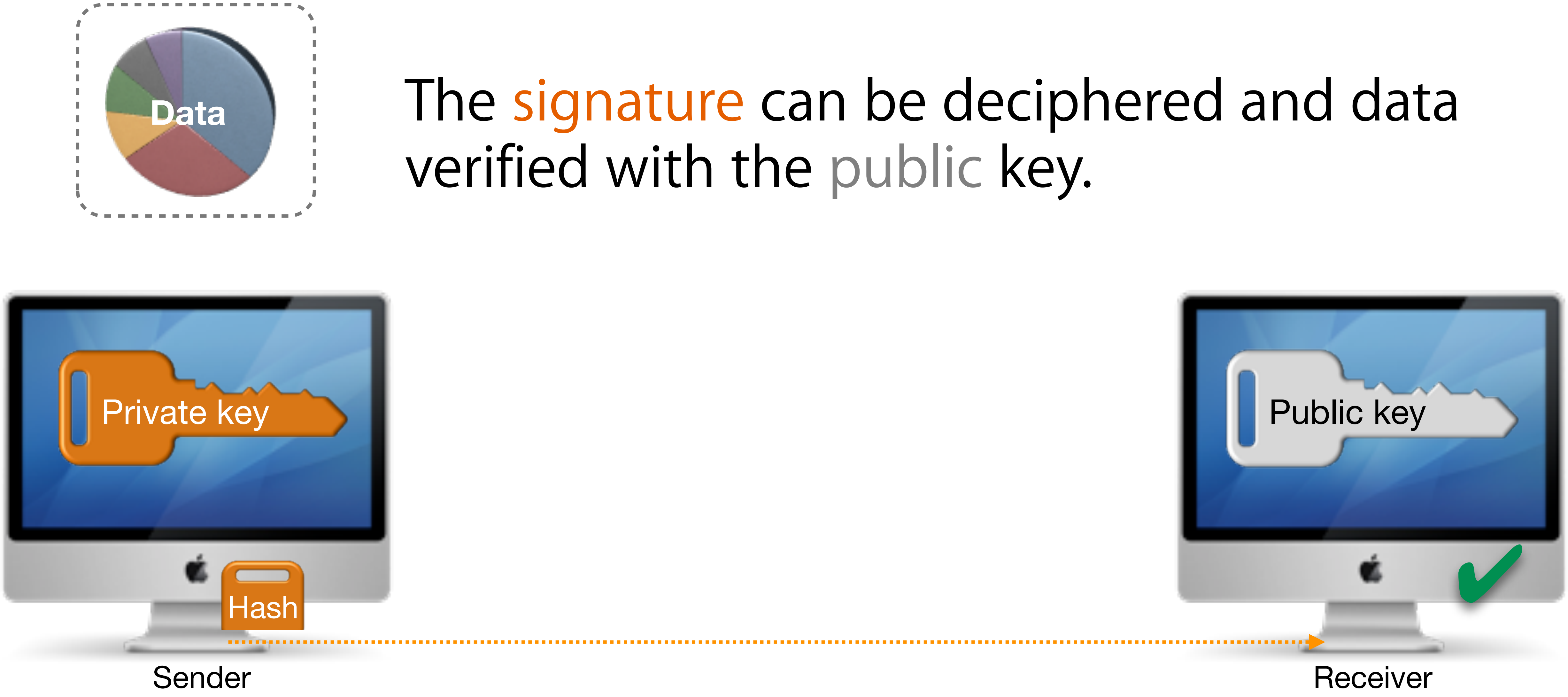
▶ **Trust**

▼ **Details**

Subject Name	
Country	US
Organization	Apple Computer, Inc.
Organizational Unit	Apple Computer Certificate Authority
Common Name	Apple Root Certificate Authority
Issuer Name	
Country	US
Organization	Apple Computer, Inc.
Organizational Unit	Apple Computer Certificate Authority
Common Name	Apple Root Certificate Authority
Serial Number	1
Version	3
Signature Algorithm	SHA-1 with RSA Encryption (1 2 840 113549 1 1 5)
Parameters	none
Not Valid Before	Wednesday, February 9, 2005 7:18:14 PM ET
Not Valid After	Sunday, February 9, 2025 7:18:14 PM ET
Public Key Info	
Algorithm	RSA Encryption (1 2 840 113549 1 1 1)
Parameters	none
Public Key	256 bytes : E4 91 A9 09 1F 91 DB 1E ...
Exponent	65537
Key Size	2048 bits
Key Usage	Verify
Signature	256 bytes : 9D DA 2D 28 58 2F 7D 76 ...

Digital Signing

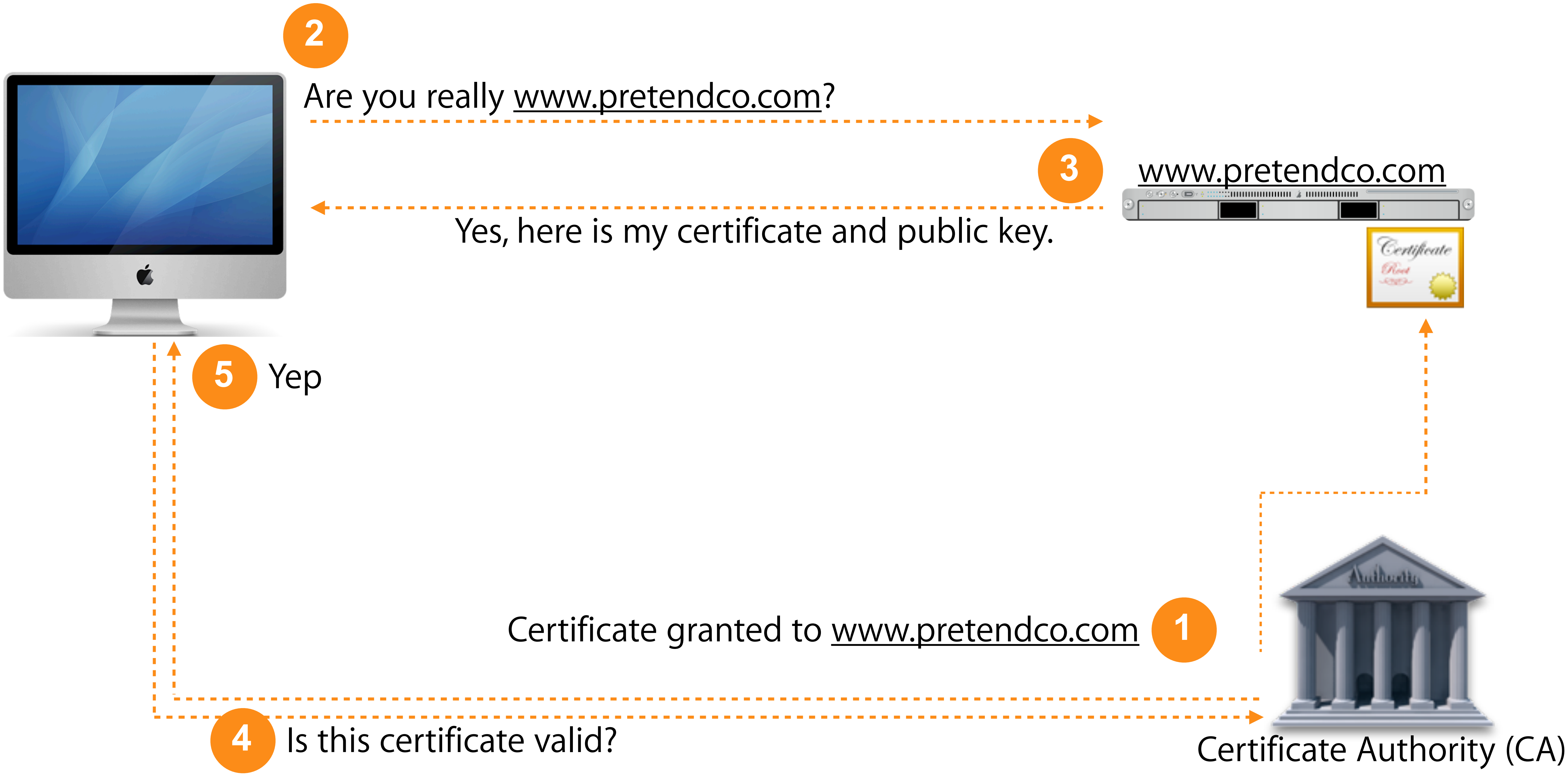
Digital signing is used to prove data has been untouched since signing.
Data is signed with a private key.



The signature can be deciphered and data verified with the public key.

Certificate Basics

Trust



2 Are you really www.pretendco.com?

3 www.pretendco.com

Yes, here is my certificate and public key.

5 Yep

Certificate granted to www.pretendco.com 1

4 Is this certificate valid?

Certificate Authority (CA)

Certificates and Services

Certificates can be used with the following services:

- Mail - POP/IMAP & SMTP
- Web - Enabled per site
- iChat
- iCal
- Podcast Producer
- Address Book Server
- Mobile Access Server
- VPN & RADIUS
- Push Notification
- Open Directory

802.1x Authentication

802.1x Network Authentication

- Authenticates wired/wireless users
- Prevents unauthorized access at network level
- Several modes and options available
- Commonly used in cell phone networks

Why Use 802.1x?

- Protects wireless from unwanted guests
- Protects wired jacks in public locations
- Dynamic VLAN switching
  - Sandboxes the user until authenticated
  - VLAN is assigned based on user or group identity in directory
- Not all switches support 802.1x

802.1x Modes

System Mode

- Provides device-level authentication
- Not user aware
- Authentication session started by the system
- Information used from System Preferences and keychain

802.1x Modes, cont.

User Mode

- Requires user credentials for network authentication
- Disconnects from network at logout
- Authentication sessions starts as user logs in
- Information from user’s preferences and keychain

802.1x Modes, cont.

Login window Mode

- Used with an external directory
- Authentication started by loginwindow
- Credentials from login window, System Preferences & Keychain

802.1x Modes, cont.

Mixed Mode

- New in Mac OS X v10.6
- Combindation of login window and system modes

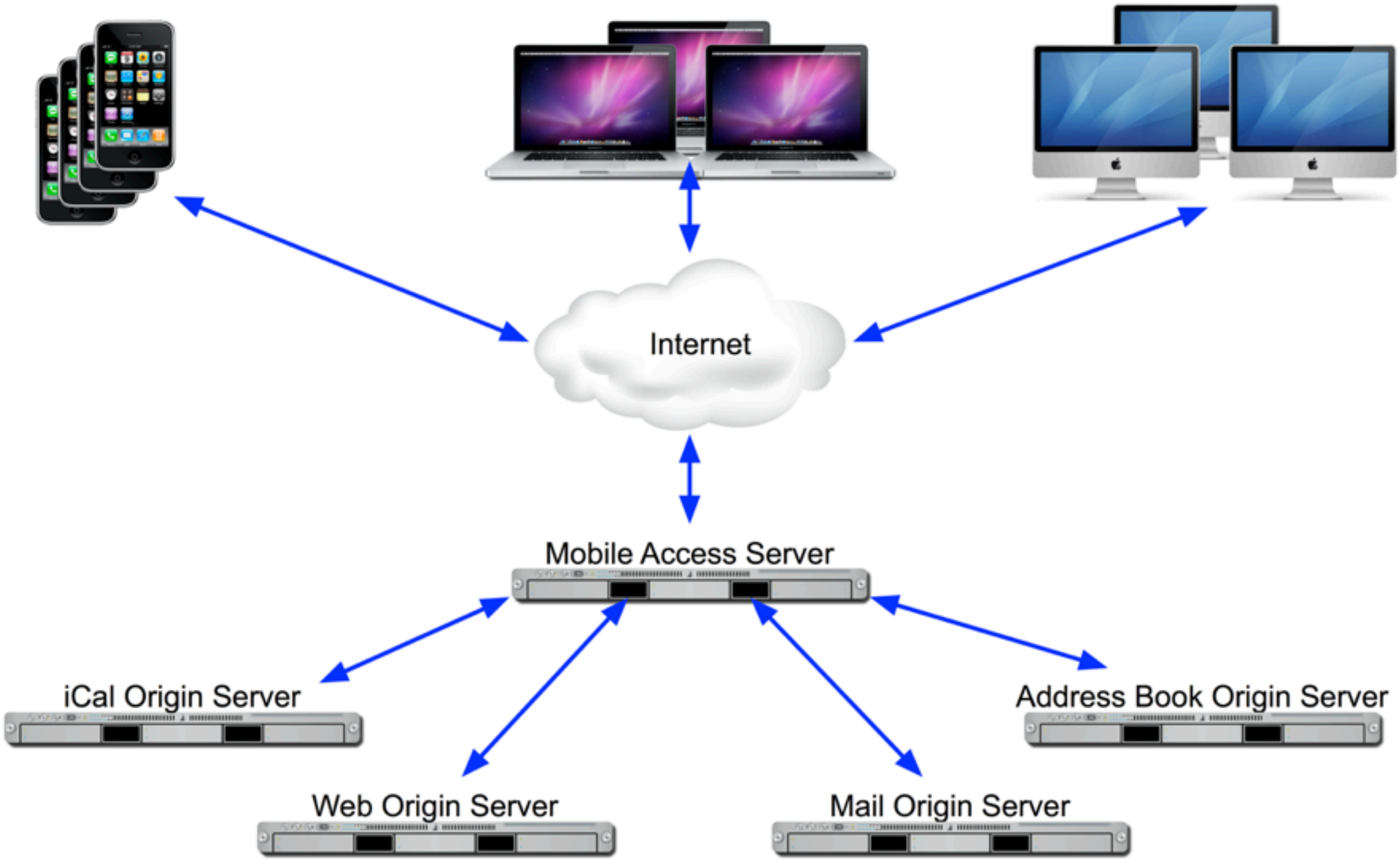
802.1x on iOS

iPhone/iPod Touch/iPad compatible

- Only System mode
- Uses profile template
- Once template is installed it provides seamless login
- Configured using iPhone Configuration Utility
- Profiles can be manually deployed via USB, emailed, or put on secure website

MOBILE ACCESS SERVER

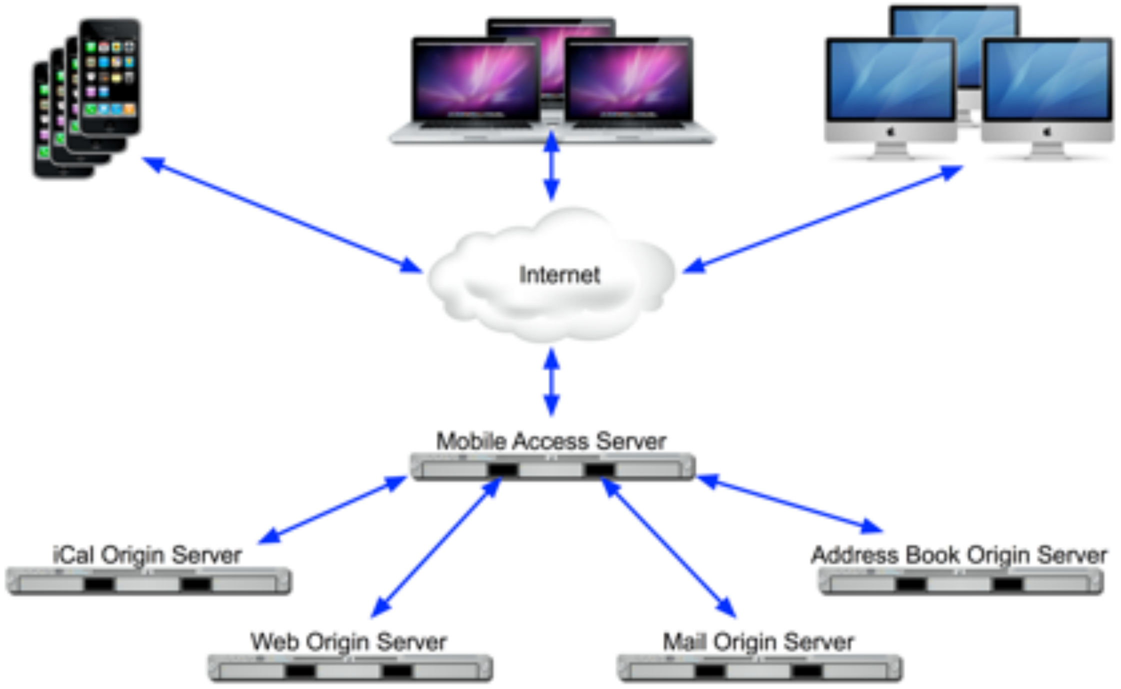
What is Mobile Access Server (MAS)?



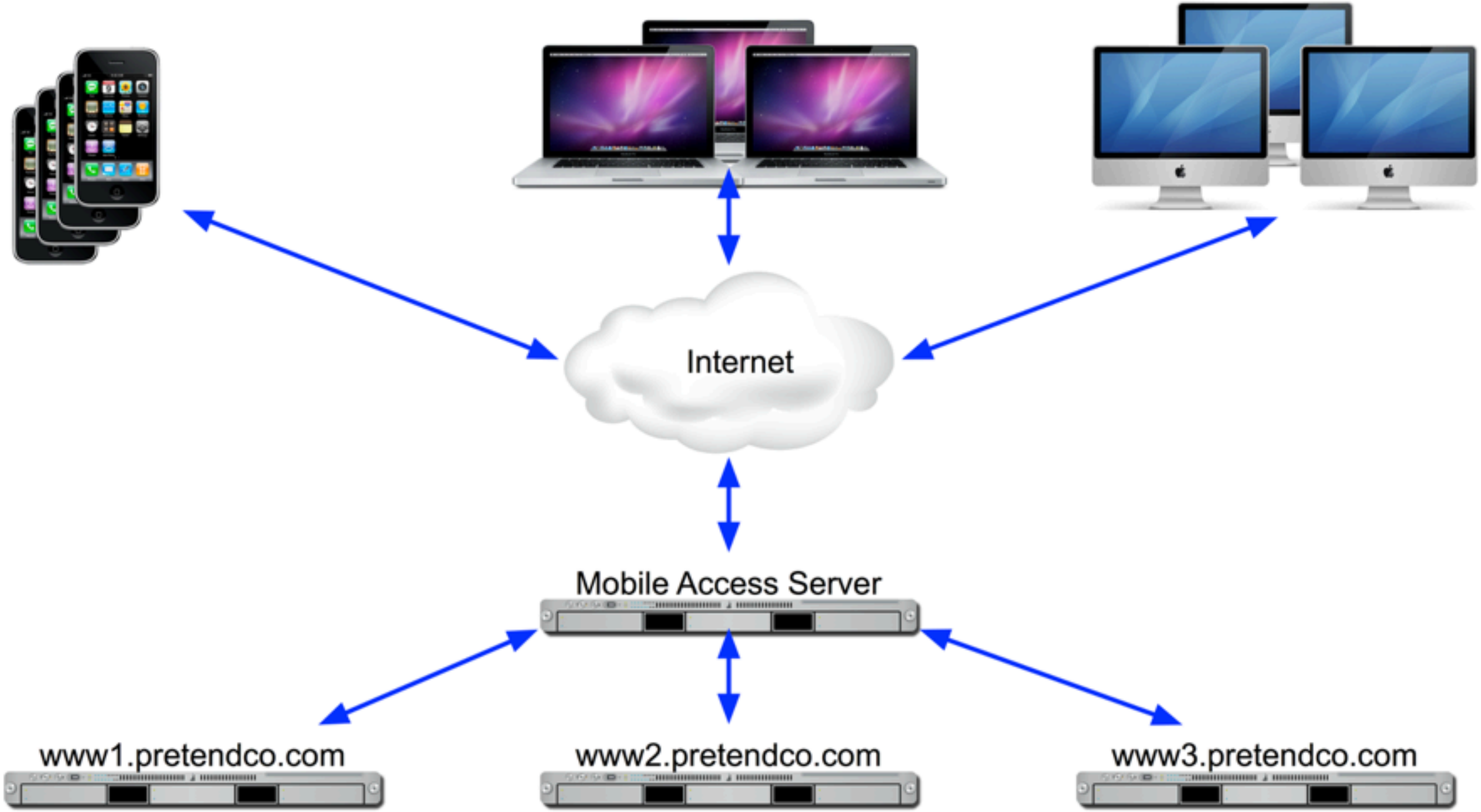
Why Use MAS?

Benefits

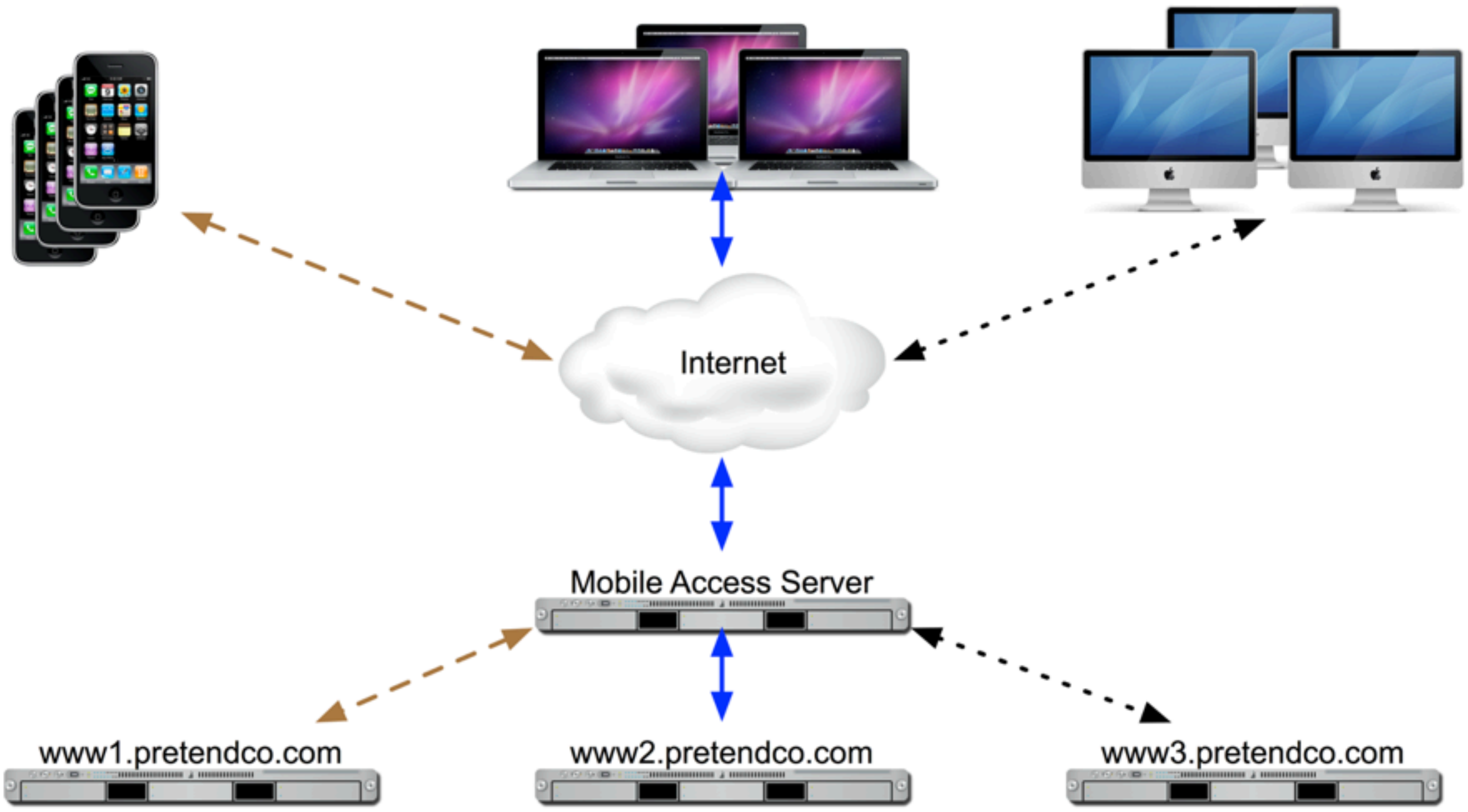
- No need to open firewall ports to allow connections to specific LAN servers
- More secure than VPN as only allows access to specific services, not entire LAN
- MAS does not host data
- MAS limits which users can authenticate and use services
- Utilizes SSL



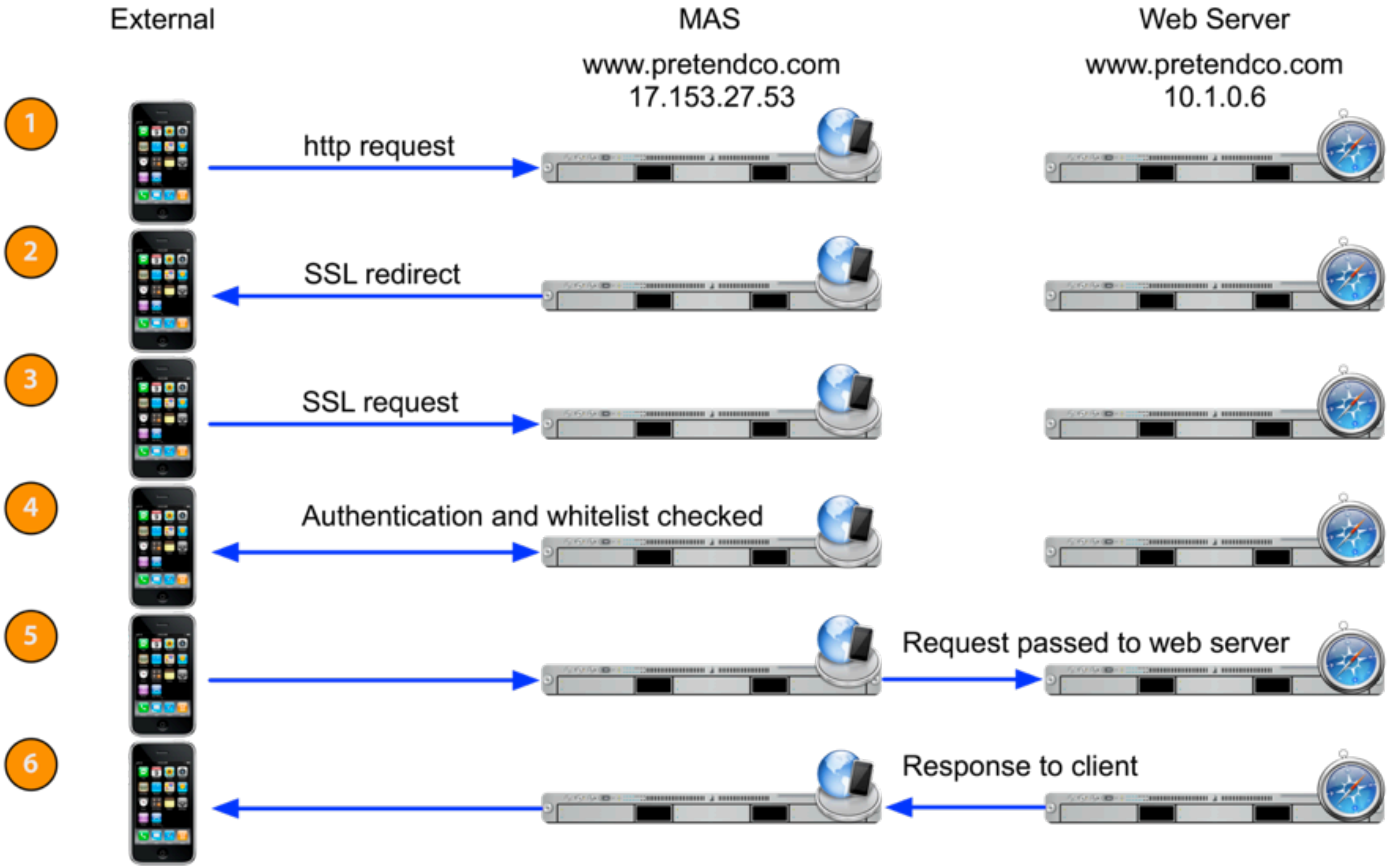
MAS and WWW (1)


Internet
Mobile Access Server
www1.pretendco.com
www2.pretendco.com
www3.pretendco.com

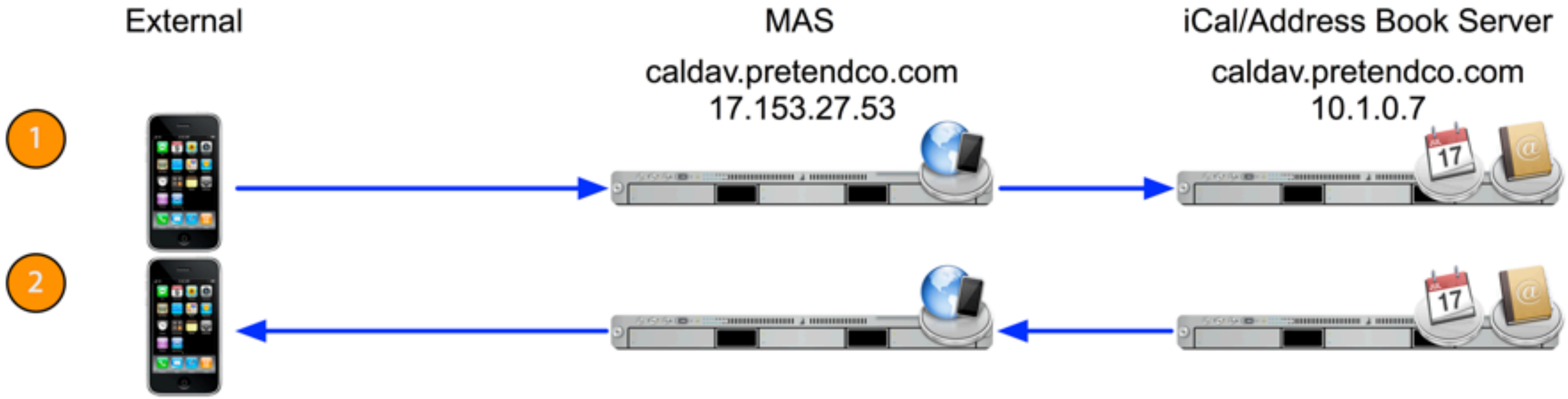
MAS and WWW (2) SNI



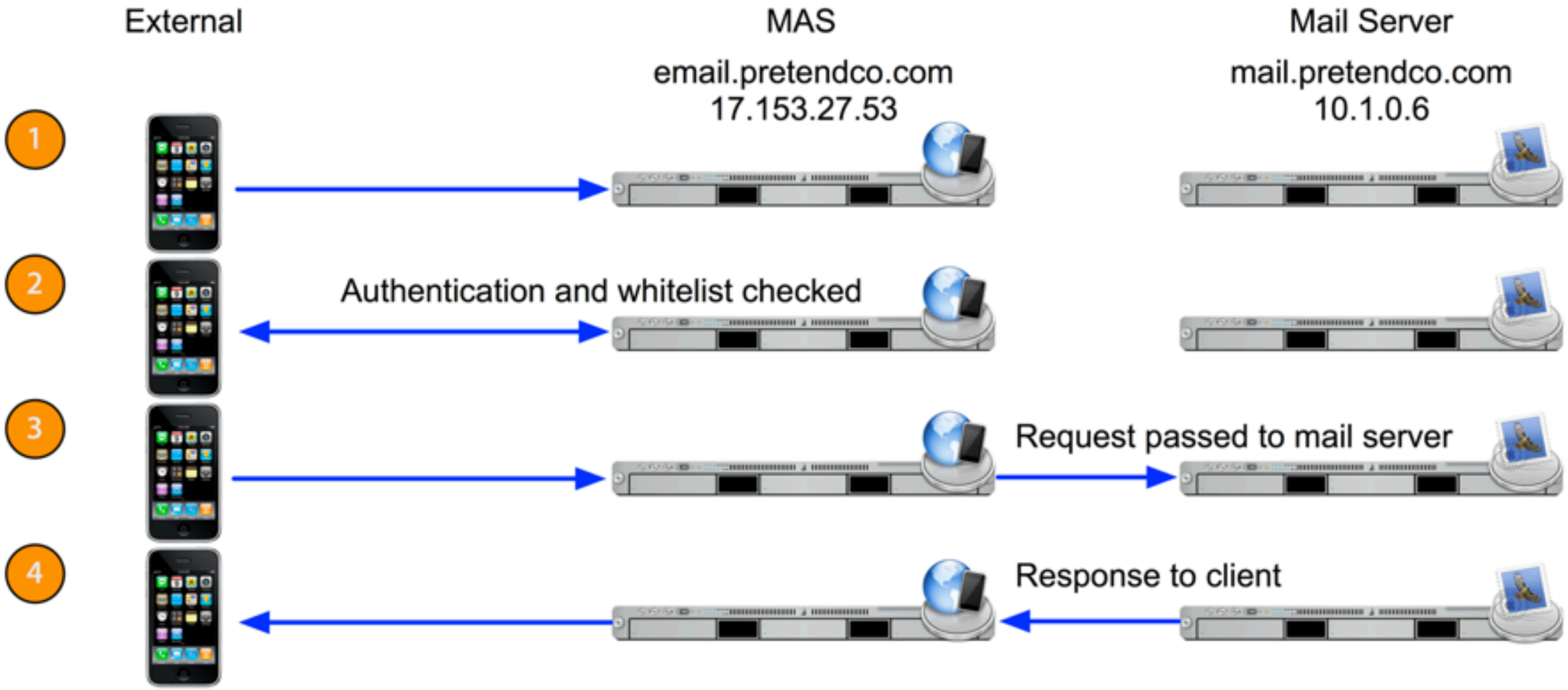
MAS and WWW


External
MAS
www.pretendco.com
17.153.27.53
Web Server
www.pretendco.com
10.1.0.6
1
http request
2
SSL redirect
3
SSL request
4
Authentication and whitelist checked
5
Request passed to web server
6
Response to client

MAS and iCal/Address Book



MAS and Mail



External

MAS

email.pretendco.com
17.153.27.53

Mail Server

mail.pretendco.com
10.1.0.6

1

2

Authentication and whitelist checked

3

Request passed to mail server

4

Response to client

Q&A