Virtual Private Cool

Session M223

Macworld San Francisco 2005

Joel Rennich

Apple Computer

Apple Certified Trainer, ACSA 10.3

Apple Certifications for 10.3.x

Course Names	Certification Level	Length (days)
Mac OS X Help Desk Essentials	ACHDS	3
Mac OS X Server Essentials	ACTC (with Help Desk Essentials)	4
System Administration of Mac OS X Clients	Apple Certified System Administrator	5 days each course
System Administration using Mac OS X Server		

train.apple.com • 800-848-6398

Virtual Private Networks

Protect your goodies!

What We’ll Cover

- VPN types
- VPN on OS X Server
- Connecting OS X to your VPN
- VPN deployments

1 VPN Types

L2TP/IPSec
PPTP
IPSec

L2TP/IPSec

- Layer 2 Tunneling Protocol over IPSec
- IPSec used to secure a “normal” PPP connection
- PPP provides user authentication
- IPSec provides security

L2TP/IPSec - Issues

- IPSec requires “modern” network
- Sometimes not usable with NAT
- Sometimes router/firewall can’t pass - might be already providing IPSec

L2TP/IPSec on OSXS

- OS X Server 10.3 built-in server
- OS X client 10.3 built-in client
- Windows 2000+
- Default VPN type for Windows 2000 and 2003 Server

PPTP

- Point to Point Tunneling Protocol
- Uses Generic Routing Encapsulation to secure a normal PPP connection
- Older VPN type

PPTP - Issues

- 40-bit version of PPTP not so great, stick with 128-bit
- Security issues in past have given it a bit of a bad reputation
- Microsoft proprietary encryption protocol - not a ratified standard

PPTP on OSXS

- OS X Server 10.3 built-in server (kind of built-in on OSXS 10.2)
- OS X client 10.2+ built-in client
- Windows 98+
- Default VPN type for Windows NT

2 OS X Server VPN

Setting up OS X Server
Setting up OS X Client

Initial Setup

- All done with Server Admin
- Users MUST have “Advanced” passwords to support VPN authentication types

Pick a Protocol

- PPTP for older clients (Win98 and 10.2) and older networks
- L2TP/IPSec for newer clients (Win2k and 10.3)

Define IP Range

- Need unique IP range for each VPN type
- Best if not in DHCP range

Configure Server

- Enable VPN types
- Assign access control group to VPN type
- Define shared secret if using L2TP/IPSec

Demo

Setting up VPN on OS X Server

Routing

- For clients to reach other systems on network through VPN, you need to turn on routing on the Server
- /etc/hostconfig set
IPFORWARDING=-YES-
- Or use sysctl:
sysctl -w net.inet.ip.forwarding=1

Routes

- Can define public/private routes for clients
- Private - clients will use VPN to access private IP range
- Public - client will use normal gateway to connect to IP range
- Defining a private implies all other traffic is public

DNS

- Regardless of public/private routes, client WILL use VPN supplied DNS server as primary DNS server
- Use DNS views to micro-manage this for VPN clients if necessary

LDAP

- To use LDAP users with VPN you MUST use vpnadduser command
- KBase article

Configure Client

- Internet Connect in Applications folder
- When you create VPN connection it will add new network interface to Network Preferences

Demo

Setting up VPN on OS X client

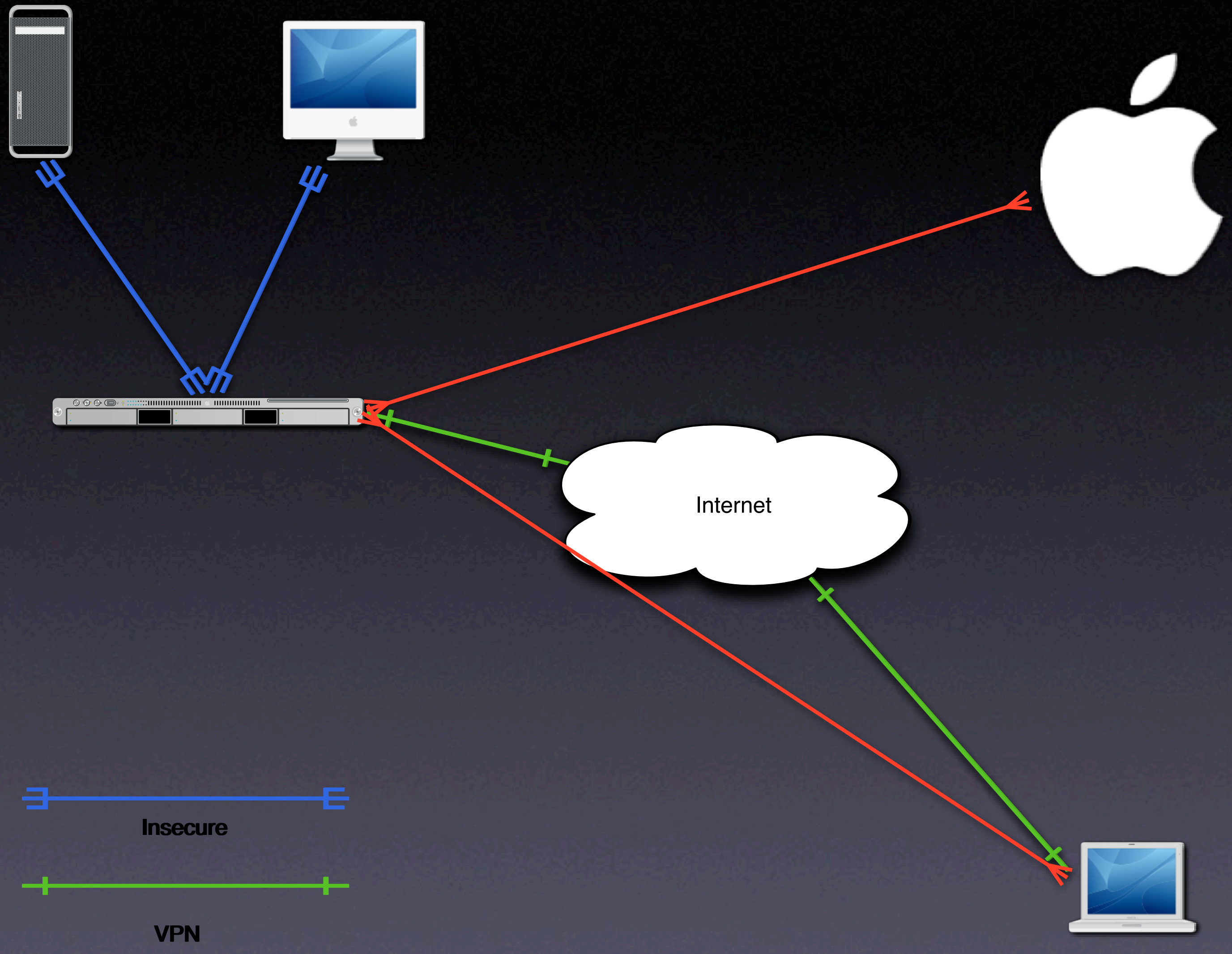
3 Deploying

Scenarios

Troubleshooting

Simple VPN setup

- All traffic goes through VPN - no public/ private routes configured
- IP forwarding configured on VPN server



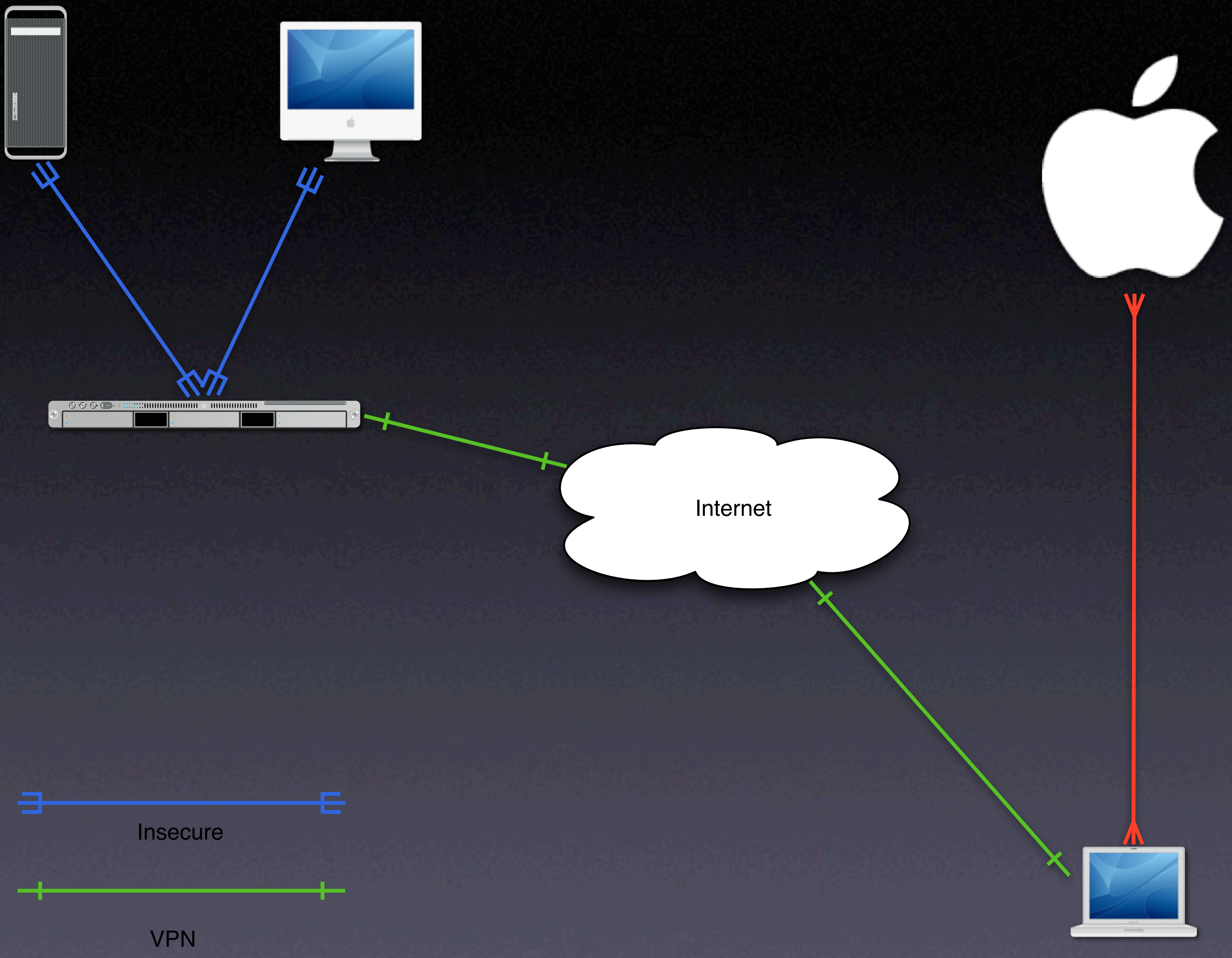
Internet

Insecure

VPN

LAN-only VPN

- Private route for VPN
- IP forwarding configured on VPN server



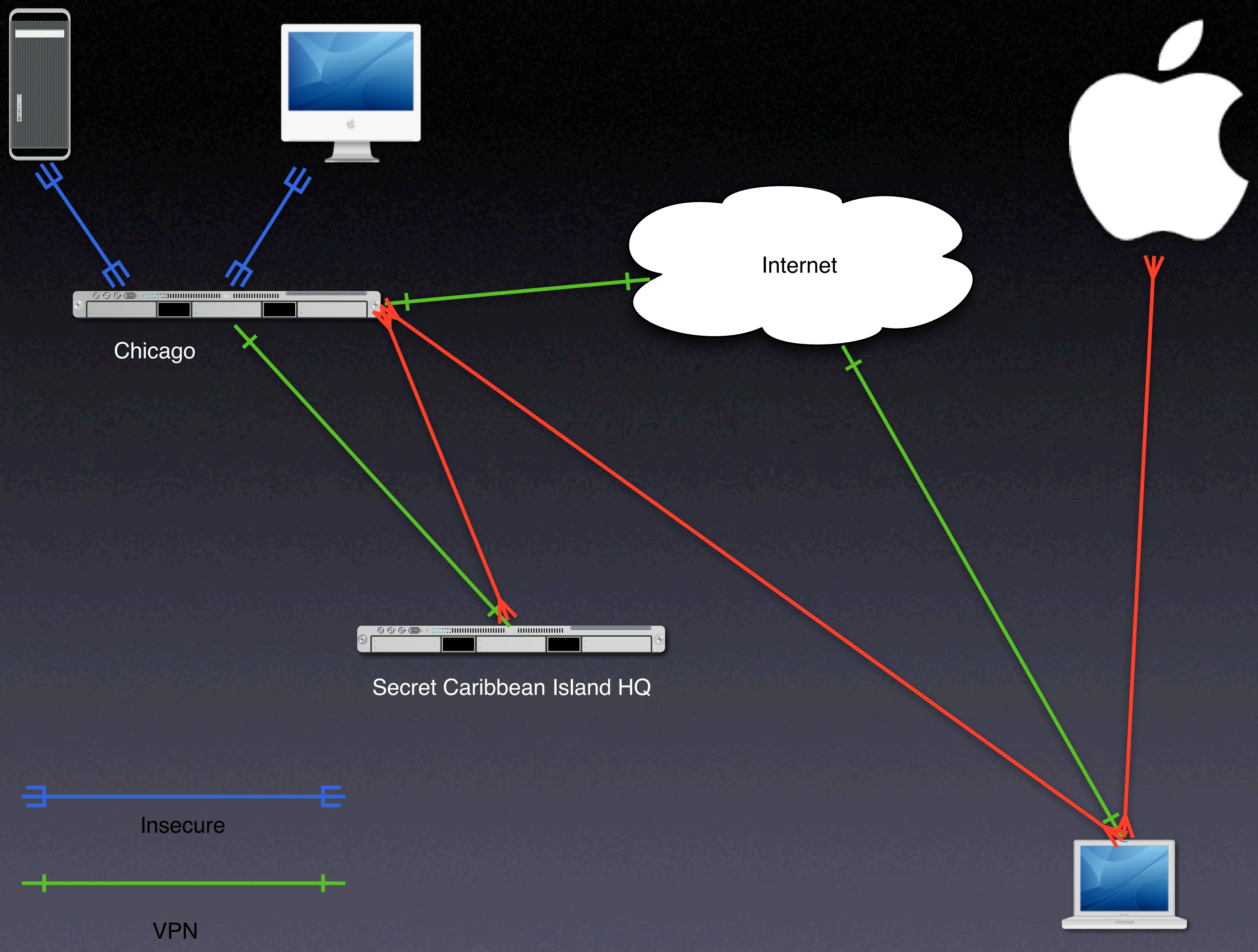
Internet

Insecure

VPN

Let’s get crazy!

- Secure LAN access with VPN
- Secure access to remote LAN with site-to-site VPN
- Allow client to use existing connection to get to rest of the Internet



Internet

Chicago

Secret Caribbean Island HQ

Insecure

VPN

Troubleshoot

- netstat - this will check routing table
- ping
- traceroute

Config Files

- /Library/Preferences/SystemPreferences/com.apple.AppleRemoteAccessServer.plist
- /etc/racoon/racoon.conf

4

Questions

Ask now

Thank You!

VPN

Session M223

Macworld San Francisco 2005

Joel Rennich

Apple Computer

Apple Certified Trainer, ACSA 10.3