Security:
Letting Them In.

MACTECH

Allen Hancock

Allen Hancock received his Bachelor's in Early Childhood Education at the University of Missouri - Columbia. This background in education keeps him coming back to speak at MacTech.

In 2000, Allen started the Mac Consulting Group, Inc: an Apple Specialist and Authorized Training Center based in Baton Rouge, Louisiana. In 2012, Allen sold the Mac Consulting Group to The Orchard, where he continue to do what he loves most: help make happy customers.

After watching too many common problems and hardware failures, Allen founded Watchman Monitoring, Inc. Its namesake product is a Software as a Service tool which allows service providers to address such problems before it's too late.

MACTECH

Why do we let people in?

- People have been known to work from home
- Some internal resources can't be opened up to the internet as a whole, but don't need security from those in the office
- Overcome technical boundaries:
  - Private domain name
  - Non-routable IP addresses
- Sometimes "in" means somewhere else.
  - Outsourced hosting providers
  - Two or more locations

MACTECH

Defining Benefits:
What do we gain with VPN access?

- Direct, fast connectivity to the network.
- Access to multiple resources which commonly use the same tcp port
  - (printers, file servers, websites, screen sharing, etc)
- Only one pinhole in the firewall
  - Behind this more secure pinhole, we can access other non-secured services
  - IPSec and L2TP over IPSec offer an additional password layer over PPTP/basic SSL VPN

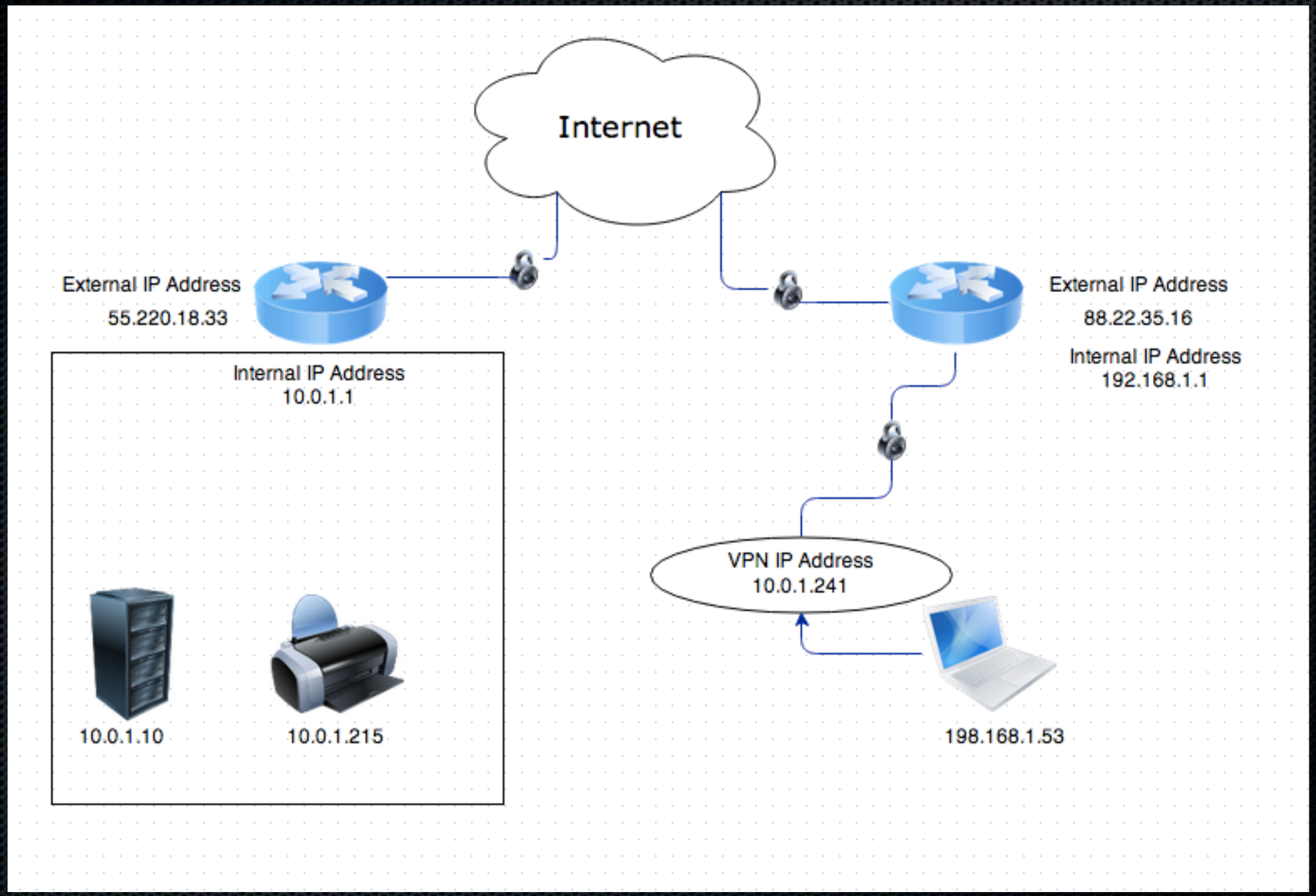
MACTECH

Benefits of a VPN(cont'd)

- Multiple layers of authentication reduce risk
- Access is easily controlled on a per-user basis
- A single set-up procedure enables access to all network resources
- Paths to network services remain constant in or out of the office
- Data Privacy at all times (at a cost)

MACTECH

Diagram of a VPN



MACTECH

Subnets matter

- Make sure the internal IP range is unique
- When both ends have matching (192.168.1.x) subnets, the computer can't know which packets belong to which end of the tunnel.

Identifying access and authorization to resources:

- How do I integrate access with authorization?
  - OS X VPN Service
    - Cisco, Juniper, etc can use OS X server for authentication via RADIUS
    - Kerio Control - offers all of the above
- Open VPN - certificate based, less password issues overall.
  http://www.dd-wrt.com/wiki/index.php/OpenVPN

Implementing a VPN Server

- Software VPN for greater flexibility
  - OS X Server's L2TP over IPSec
  - OpenVPN
  - Hamachi (quasi-vpn)
  - Pertino
- Hardware VPN for greater reliability
  - Cisco, Sonicwall, Kerio, PFSense etc etc etc

OpenVPN

- Port Forwarding
  - UDP 1194
  - TCP 943 change to 443 for greatest access
- iOS App- OpenVPN Connect
  - https://itunes.apple.com/app/openvpn-connect/id590379981
- Mac App-Tunnelblick
  - https://code.google.com/p/tunnelblick/

MACTECH

Why not PPTP?

- Traditional answer
  - it's cracked - true for an implementation from Microsoft, not universally true
  - It's inherently less secure due to a lack of second factor authentication.
    - If opening up a port to an AFP File server is bad because it's just a username & password away, PPTP is potentially going to allow access to the entire LAN

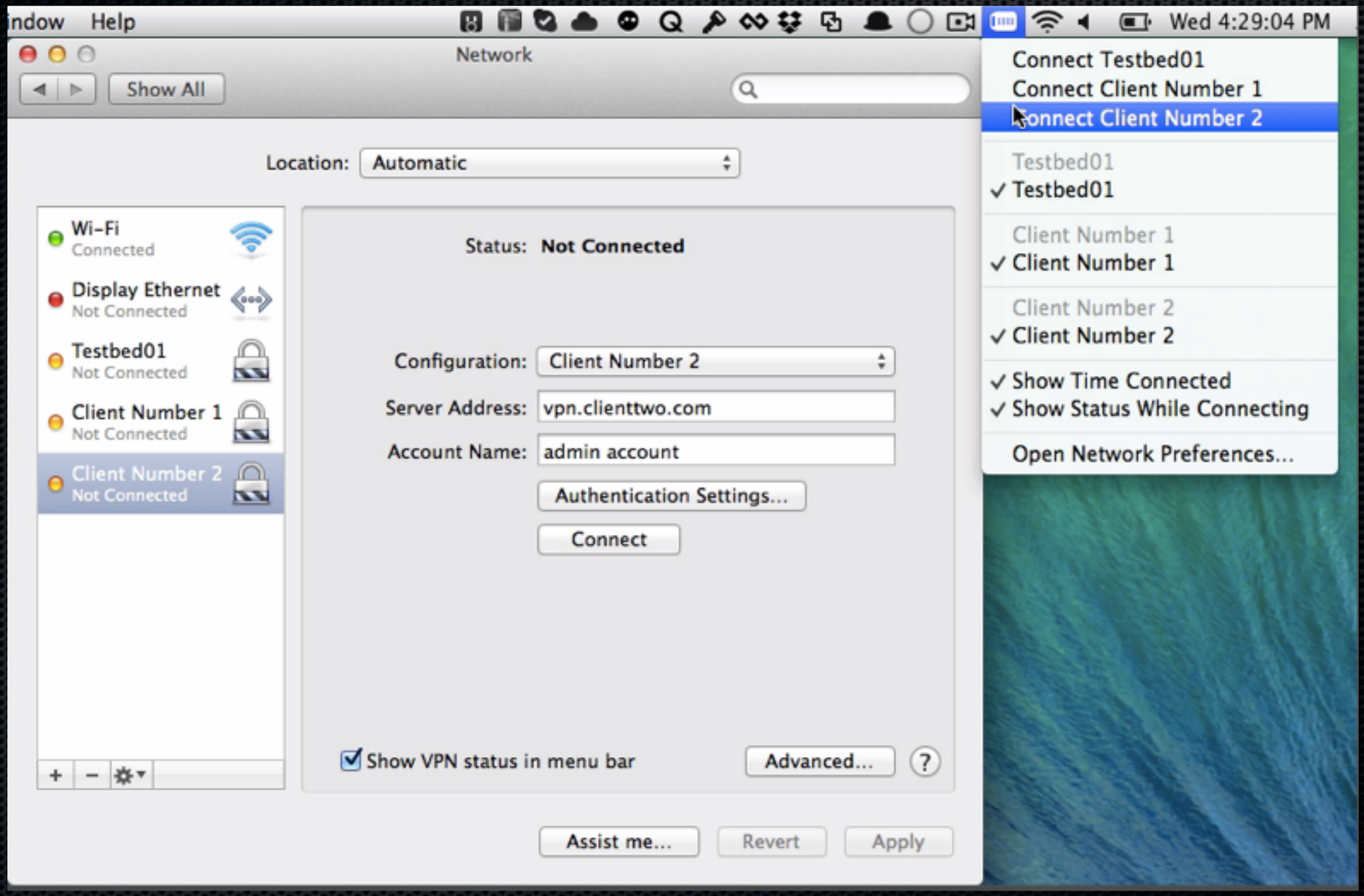
Write it all down

- Document what access you've implemented.
- Standardize storage of VPN configurations
- Deploy with iPhone Configuration Utility
  - Works with iOS and Mac OS X 10.7+

Configuration Utility

- Tap on Configuration Profile
- Click New
- Assign a useful Profile Name
- Identifier: CompanyDomainName.vpnprofile
- Tap VPN
- Tap Configure
- Enter Connection Name (matches profile name)
- Enter Connection Type: L2TP for Mac OS X Server
- Enter the Server's IP address or host name
- The Account Name: leave blank as this will be set on a per-computer basis
- Choose Export; Save the resulting file to a Utilities folder on the file server
- The resulting mobile config file can be imported onto any recent MAC or iOS device

Keeping a sane VPN list



MACTECH

Don’t get locked out

- How do you allow yourself (admin) to get in from outside when there are issues?
- Network level vpn (Don’t cross the ports)
- Backup remote access to a dedicated computer

Resources

- https://yesthatallen.com/mactech-vpn-notes/
- http://ook.co/blog/configuring-cisco-ios-to-authenticate-vpn-users-with-open-directory/
- http://krypted.com/tag/configure-mac-os-x-server-as-a-vpn-server/
- http://radiotope.com/content/sonicwall-opendirectory-user-authentication

MACTECH

Questions?

Allen Hancock
Founder
watchman@watchmanmonitoring.com

MACTECH