IT825: Using OS X Server's Firewall

Sara Porter
Mike Sebastian

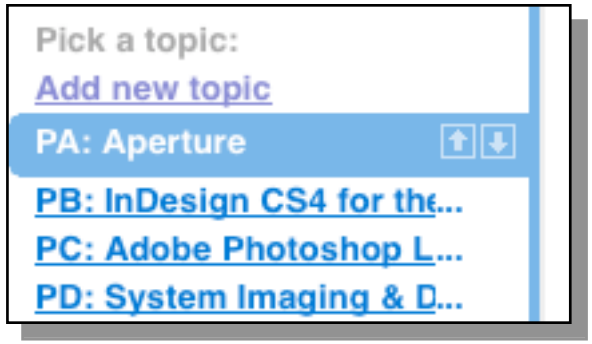
IT825: Using OS X Server's Firewall

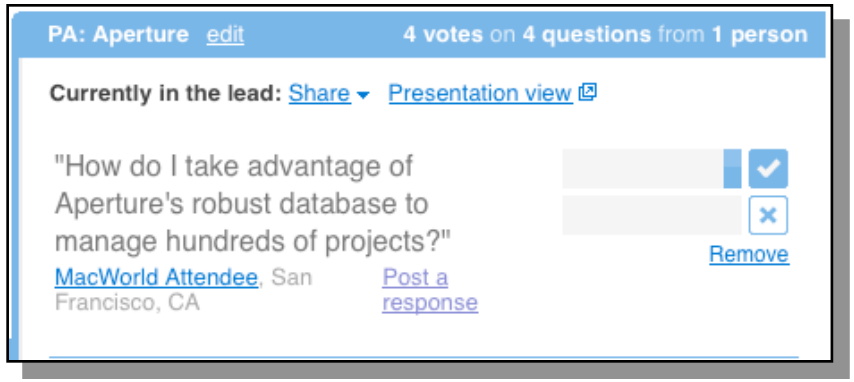
Sara Porter
Mike Sebastian

Q&A – MacIT® Conference

We are using Google Moderator to take questions for this session.

1. Go to http://tinyurl.com/633v6e
2. Pick the topic that matches this session
3. Sign in using a Google Account
   User Name: <Your Google Name>
   Password: <Your Password>
4. Submit the questions you want to ask
5. Vote on others' questions you want answered





What is a Firewall?

- A geeky movie starring Harrison Ford (Han Solo).

What is a Firewall?

- A geeky movie starring Harrison Ford (Han Solo).

What is a Firewall?

- A firewall is an integrated collection of security measures designed to prevent unauthorized electronic access to a networked computer system.
- It is also a device or set of devices configured to permit, deny, encrypt, decrypt, or proxy all computer traffic between different security domains based upon a set of rules and other criteria.

Not All Firewalls are Created Equal

Packet Firewalls

- Inspecting packets, one by one
- Allow / Deny based on rules

Stateful Firewalls

- Any firewall that performs stateful packet inspection (SPI) or stateful inspection
- Keeps track of the state of network connections traveling across it.
- Programmed to distinguish legitimate packets for different types of connections.
- Only packets matching a known connection state will be allowed by the firewall; others will be rejected.

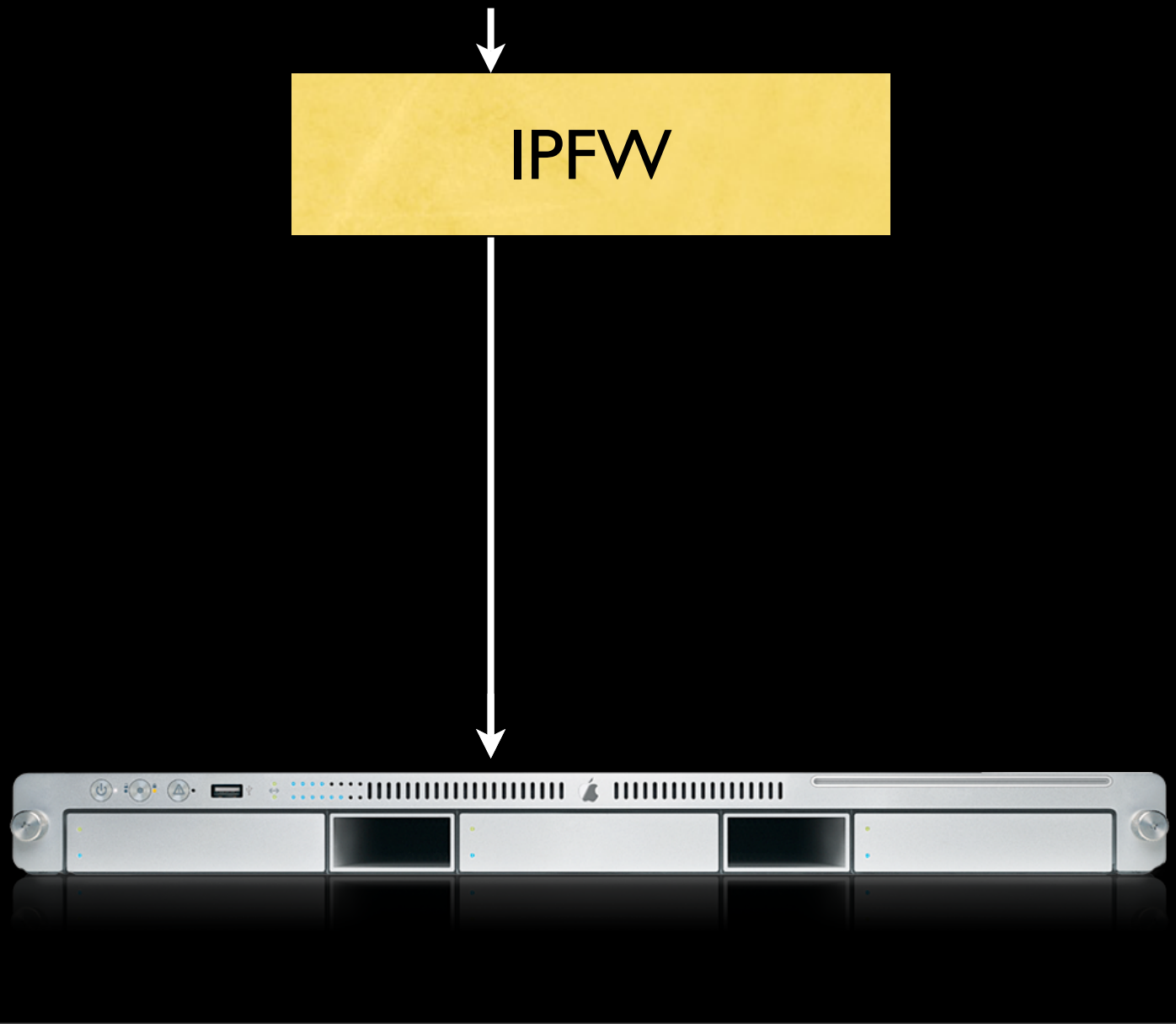
Ports

- Common ports
  - http://support.apple.com/kb/TS1629?viewlocale=en_US
  - Internet Assigned Number Authority
    - http://www.iana.org/assignments/port-numbers

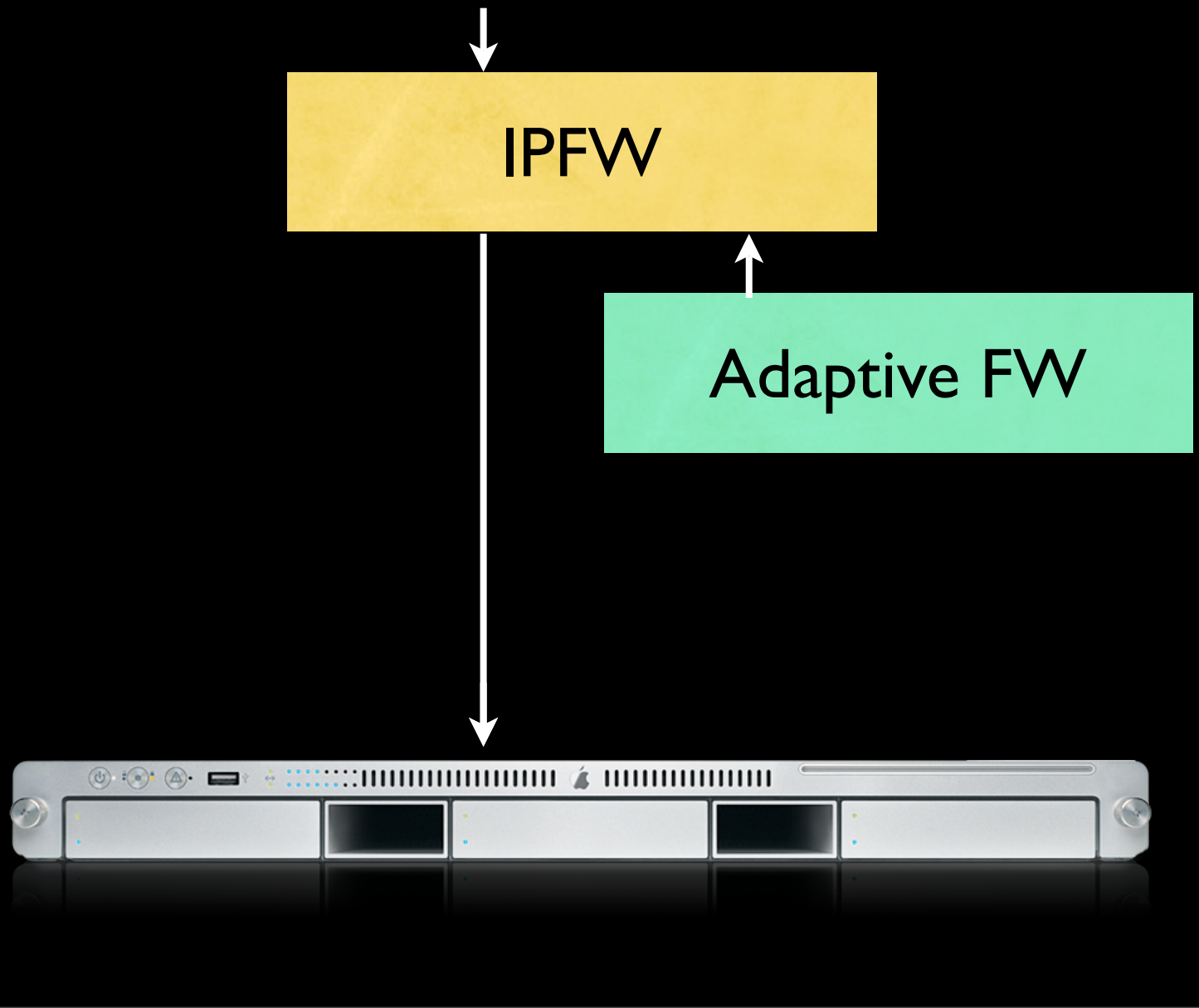
OS X Leopard

Data coming into server

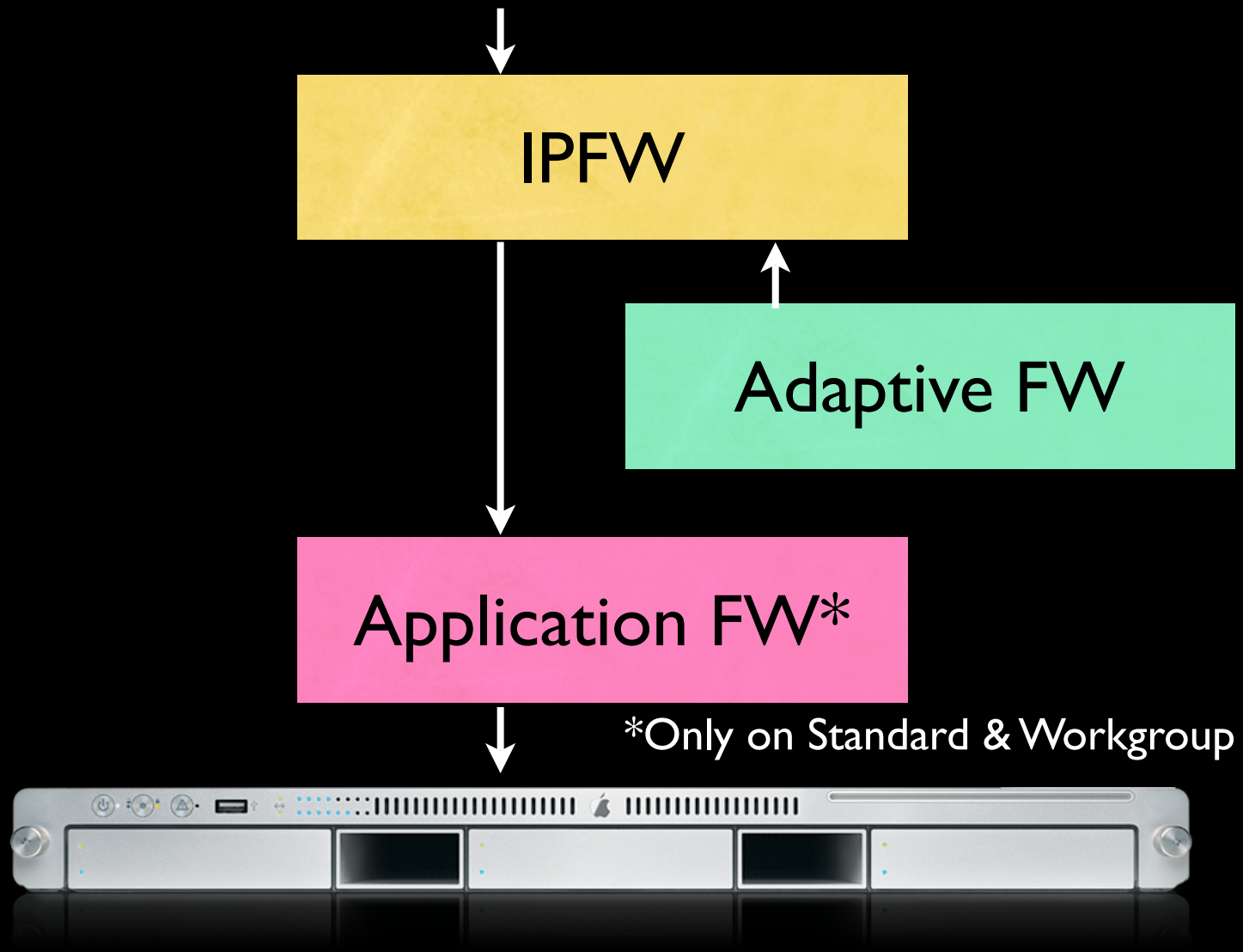
OS X Leopard



OS X Leopard



OS X Leopard


IPFW
Adaptive FW
Application FW*
*Only on Standard & Workgroup

IPFW

- Packet Based
- Plan your Firewall out first before clicking apply - because it's instant for all connections, and if you forget to enable the FTP port, then you've just cut out FTP access...
  - Think before you click!

Implementation

- Rules are created
- Services attempt to talk to the Server
  - Service is run against the rule set
  - First rule to match wins, and it stops
  - If no rules match, hits default rule of (usually) drop

Common Services

- Web
  - Enabled internally and externally
- FTP
  - Enabled internally and externally (probably)
- Mail
  - Enabled internally and externally

Common Services

- File services
  - Enabled internally only, available from external only via VPN
- Print services
  - Enabled internally only, available from external only via VPN

Change control

- Document, document, document!
- Know what you are blocking
- Ensure a change control process before any firewall changes can go into effect!

Starting the Firewall

- GUI
  - Server Admin
  - Open the Services
  - Select Firewall
  - Click Start Firewall
- Command line
  - sudo serveradmin start ipfilter

Servers

- Xserve
  - 2 Network Interfaces

Servers

- Network 1
  - Private IP
  - 192.168.1.x
- Network 2
  - Public IP
  - 17.149.160.10

Servers

- Network 1
  - Private IP
  - Internal Office
- Network 2
  - DMZ
  - Web/Mail/FTP

Firewall

IP Address Groups

- Simultaneously set firewall rules for large numbers of network devices
- By grouping IP addresses you can simultaneously set firewall rules for large numbers of network devices and allow for much better organization. This enhances the security if your network.

IP Address Groups

- By default, an IP address group is created for all incoming IP addresses.
  - The Any group
- Rules applied to this group affect all incoming network traffic.

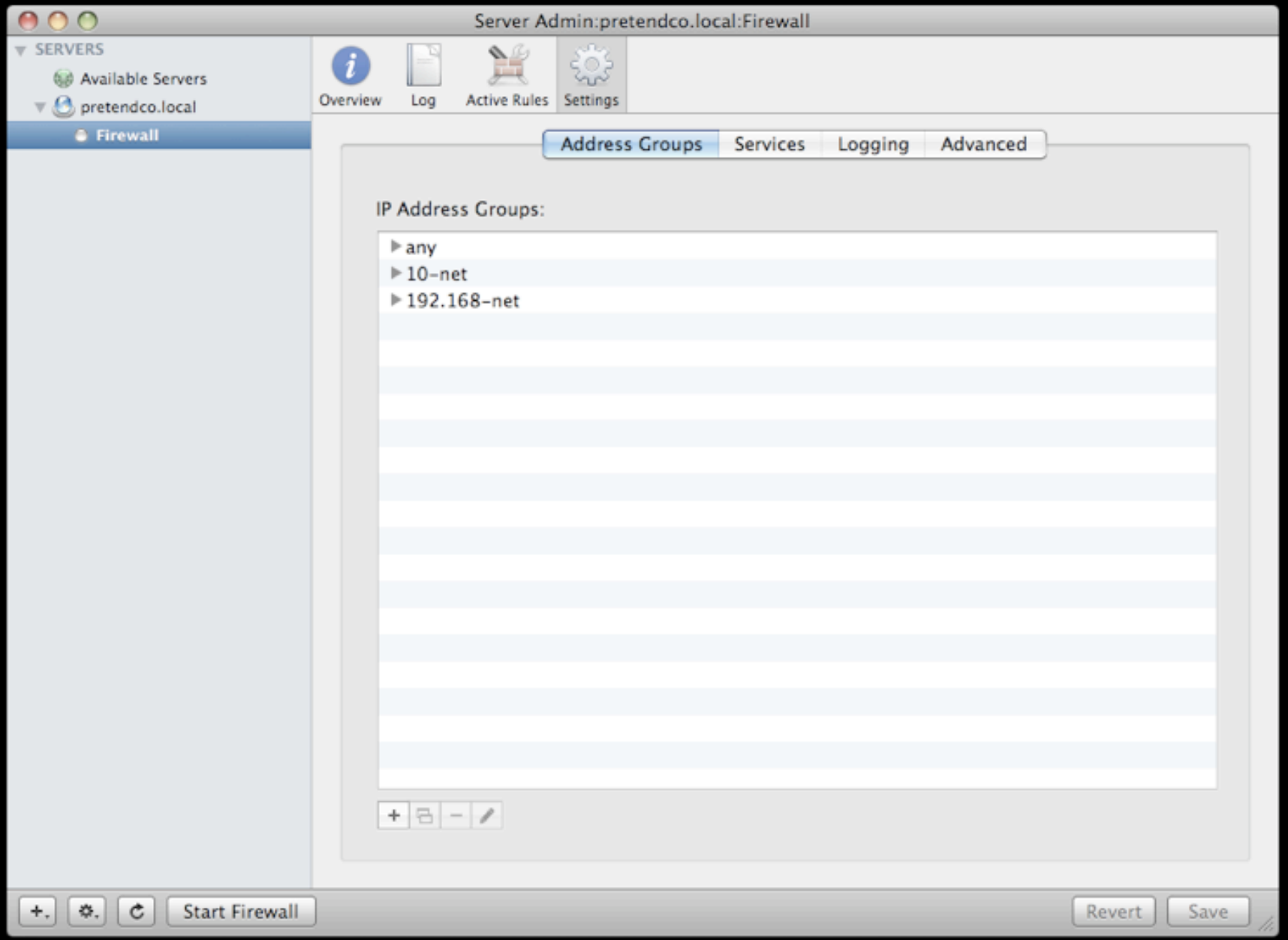
IP Address Groups

- If you add or change a rule after starting Firewall service, the new rule affects connections already established with the server.
- For example, if you deny all access to your FTP server after starting Firewall service, computers connected to your FTP server are disconnected.

IP Address Groups

- Creating Firewall Service Rules By default, Firewall service permits all UDP connections and blocks incoming TCP connections on ports that are not essential for remote administration of the server.
- Also, by default, stateful rules are in place that permit specific responses to outgoing requests.
- Before you turn on Firewall service, make sure you've set up rules permitting access from IP addresses you choose; otherwise, no one can access your server.

Server Admin



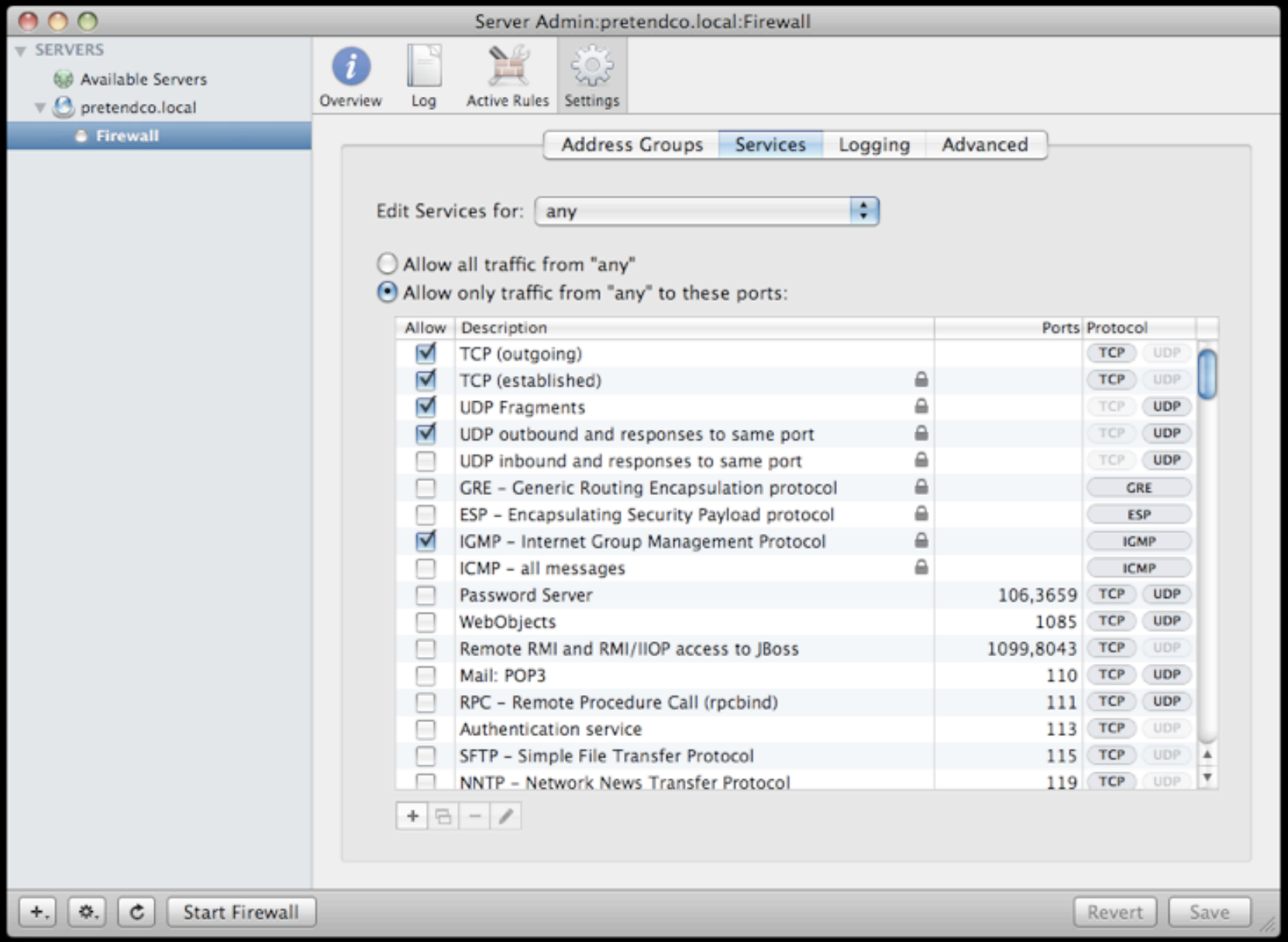
Services

- You can easily permit standard services through the firewall without advanced and extensive configuration. Standard services include:
  - SSH access
  - Web service
  - Apple File service
  - Windows File service
  - FTP service

Services

- Printer Sharing
- DNS/Multicast DNS
- ICMP Echo Reply (incoming pings)
- IGMP
- PPTP / L2TP VPN
- QTSS media streaming
- iTunes Music Sharing

Server Admin



Command Line

- Common commands
  - ipfw list
  - man ipfw
  - sysctl -w net.inet.ip.fw.enable=1

Command Line

- ipfw add deny dst-port 548 via en0
  - block AFP on en0
  - Add - denotes adding a rule
  - deny - indicates what type of rule
  - dst-port - which port the rule affects and specified b number or service name
  - via - the packets arriving via specified interface or IP address

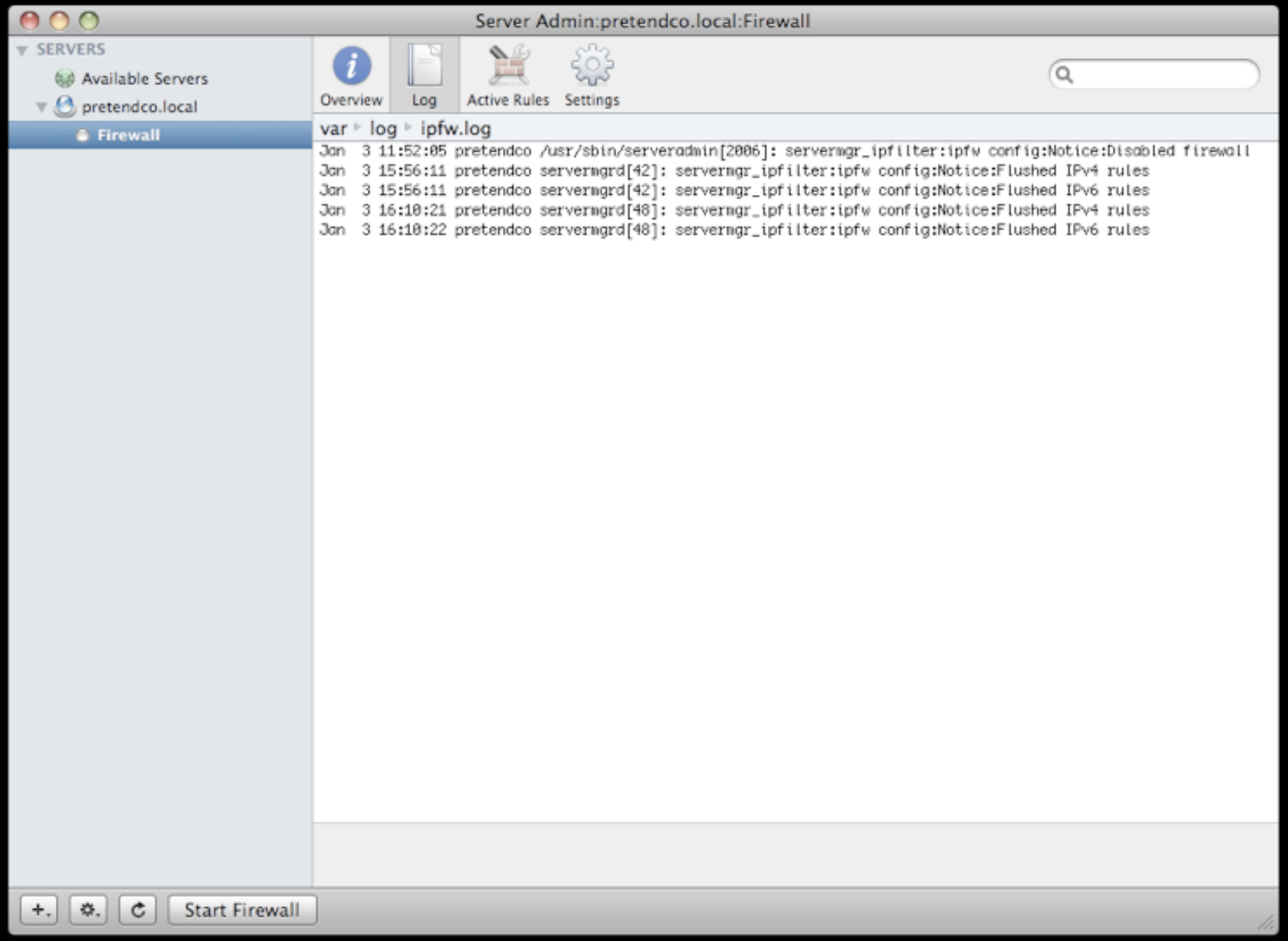
Command Line

- If a number isn't specified, ipfw will assign a default number to the rule - which will be the last rule but one (the default rule). Also makes deleting the rule much easier later if it's no longer necessary.
- ipfw add 6000 deny dst-port 548 via en0
  - Specifies the rule number
- ipfw del 6000

IPFW Log

- Log located at /var/log/ipfw.log

Server Admin



IPFW Log

- Each entry follows form:
  Nov 17 09:50:45 <hostname> ipfw[1940]: 2050 Deny TCP 192.168.1.45:49232 17.168.7.18:548 in via en0
  - Time of entry: Nov 17 09:50:45
  - Host: <hostname>
  - Process name and ID: ipfw[1040]
    - Log message: None above

IPFW Log

- Nov 17 09:50:45 <hostname> ipfw[1940]: 2050 Deny TCP 192.168.1.45:49232 17.168.7.18:548 in via en0
  - Matching rule number: 2050
  - Action: Deny
    - Could be Deny, Accept, etc
  - Protocol: TCP
    - Could be UDP, TCP, etc

IPFW Log

- Nov 17 09:50:45 <hostname> ipfw[1940]: 2050 Deny TCP 192.168.1.45:49232 17.168.7.18:548 in via en0
  - Source: 192.168.1.45:49232
  - Destination: 17.168.7.18:548
  - Interface: in via en0
    - Could be lo0(loopback), en1, etc

Adaptive Firewall

- Have you been having strange problems with your OS X Server?
- If you type the wrong AFP password, do you lose all contact with your server for ~15 minutes?

- Are you temporarily firewall'd?

Adaptive Firewall

- As it turns out, OS X Server 10.5 has two firewalls.
- The primary one you see in the Server Admin, and a second one, that turns on whenever you turn on the primary one.
- The second one is called the Adaptive Firewall. It has no controls or options via the GUI.

Adaptive Firewall

- Not really a firewall per se, but a monitoring service

Adaptive Firewall

- Scrapes the logs and creates rules based on failures (IPFW)
- No GUI to manage

Adaptive Firewall

- Supposed to firewall IP's after 10 failed login attempts
- Earlier versions of OS X Server are buggy and can block AFP after one failed, and SSH after 3; FTP can also be odd as it's log scraping and depending on how often FTP failures are logged can increase the amount of "perceived" failures.
- /var/log/secure.log scraped for internet

Adaptive Firewall

- Apple Event Monitoring daemon, emond performs actual monitoring and drives Adaptive Firewall into action

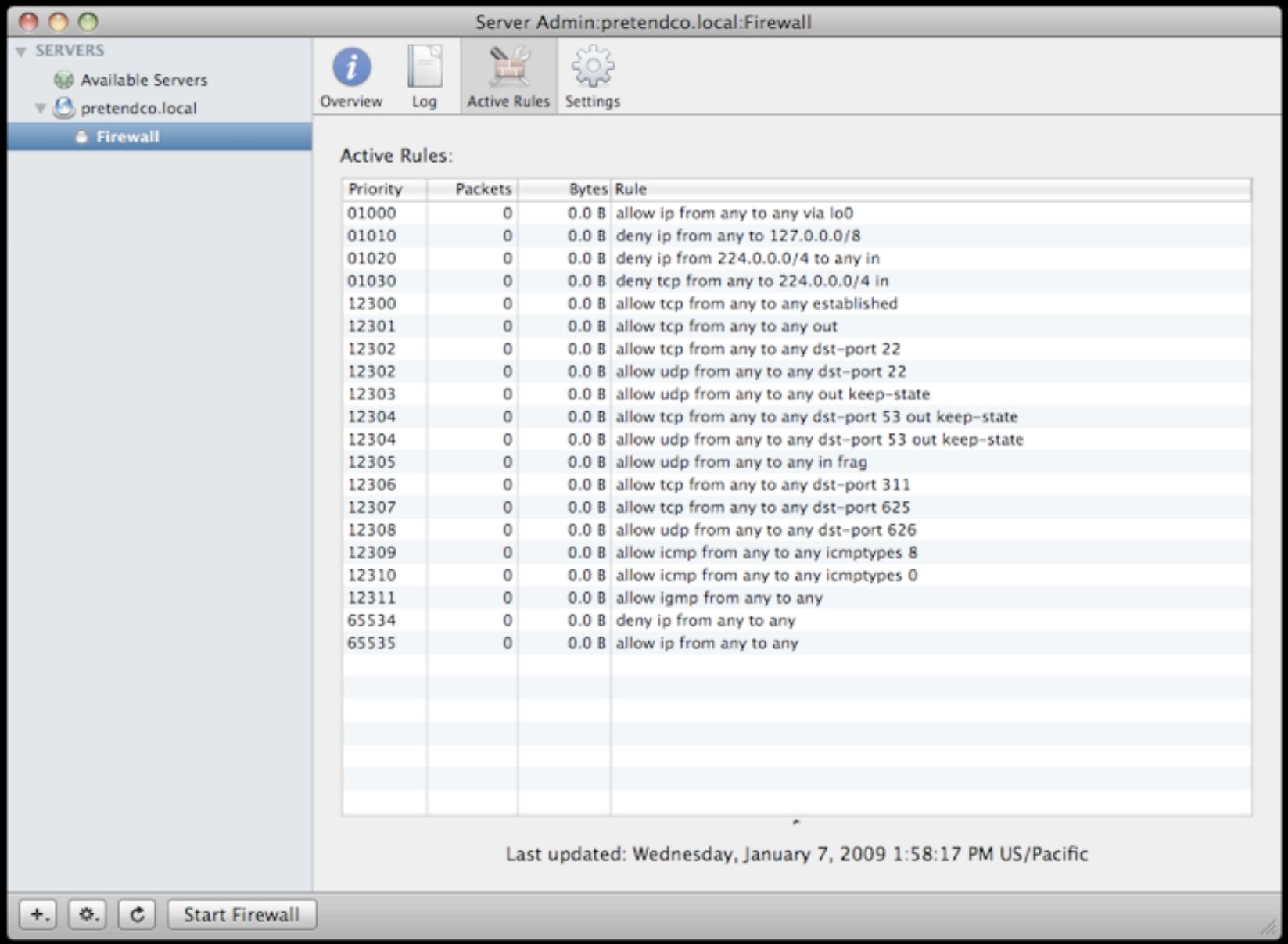
Adaptive Firewall

- emond is itself an off-limits subsystem, the man page states:
  "emond accepts events from various services, runs them through a simple rules engine, and takes action"
- And one of its rules is /etc/emond.d/rules/AdaptiveFirewall.plist which is activated on too many failed login attempts

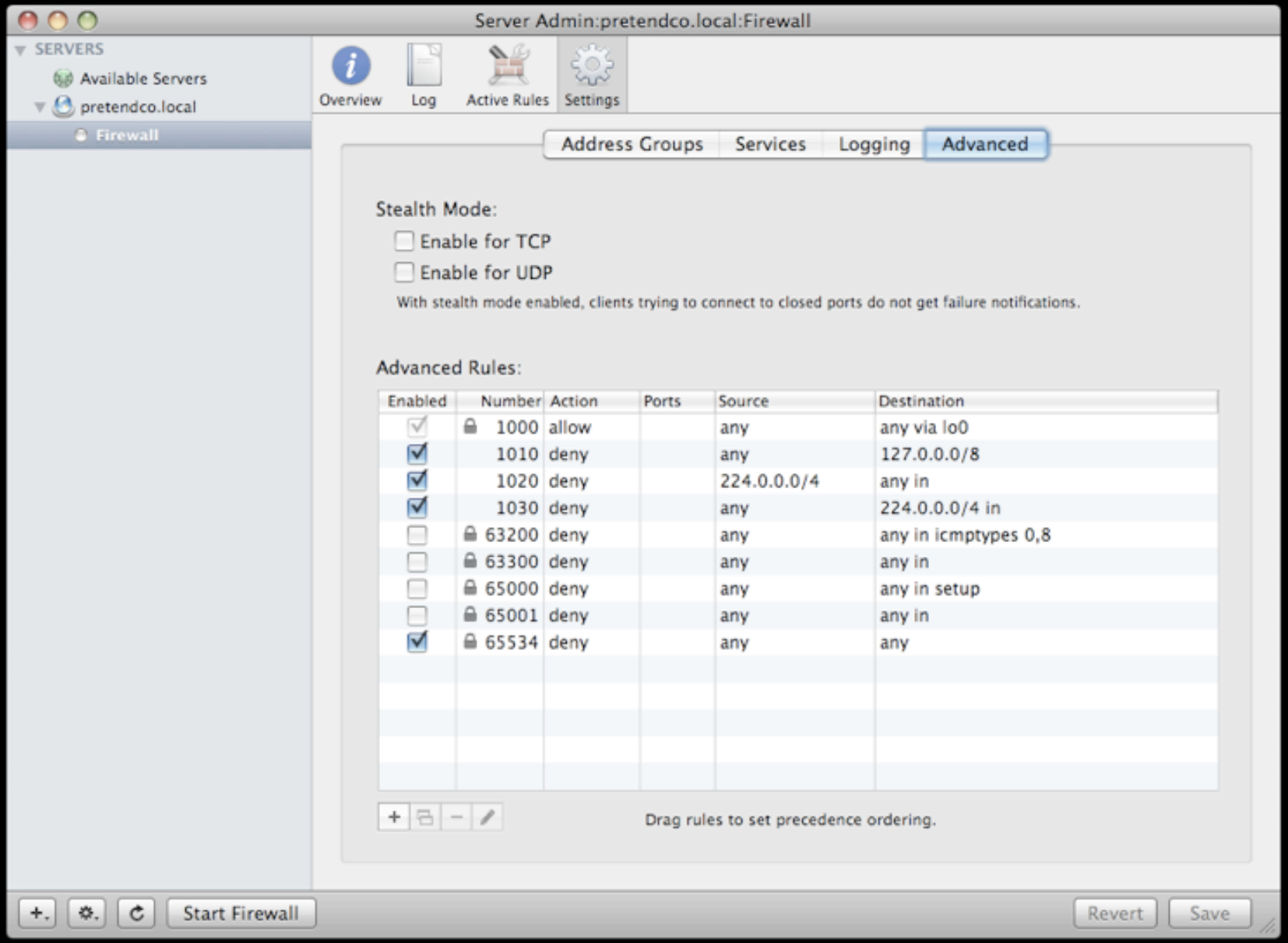
Adaptive Firewall

- But what it is supposed to do, is firewall users IPs for 15 minutes after 10 failed login attempts.
- What it DOES do is firewall IPs for 15 minutes after ONE failed AFP login attempt. Or 3 SSH attempts.

Server Admin



Server Admin



Adaptive Firewall

- This malfunction actually can work out well, as there are few AFP users so why not be super tight with security.
- But for most servers, this bug is going to be a serious pain.
- The only way to turn this feature off through the GUI is to turn off the firewall all together.

Adaptive Firewall

- Obviously not a great idea.
- So here is a way you can hack the system and manually turn off the Adaptive Firewall:
  - Open the file (as root): /etc/emond.d/rules/AdaptiveFirewall.plist

    Find the '<key>Active</key>'
    Then on the next line, inside the '<string>' tags, change the 1 to a 0

Adaptive Firewall

- Save the file and close it, and you're done.
- Now just stop and start the firewall and the service should be gone.
- You can test it by trying to connect to your server via AFP. Use the wrong password on purpose. If it asks you to re-enter it, the Adaptive Firewall is gone.
- If you lose all contact with your server, it's still running.

Adaptive Firewall

- Another way to verify what is going on is to have a test system
- Connect with a bad password from the test system. Find the IP on the test system (via System Prefs). Then look at the Firewall in Server Admin on the server.

Adaptive Firewall

- You'll be able to see a new rule that blocks the test system.
- These rules auto-delete after 15 minutes.
- Its a nice feature, it just needs to work the way its supposed to, and you need to be able to customize it.

Adaptive Firewall

- The adaptive firewall kicks in differently for different classes of services. For ftp & ssh it looks at log scrapings from /var/log/secure.log and counts each auth failed message as a "strike".
- For other services, such as AFP & mail, it gets info from the password server, again each failure there counts as one "strike".
- Unfortunately ssh and ftp tend to spit out several log messages when they get an auth failure, this makes the adaptive firewall system hypersensative to those services.

Adaptive Firewall

- The earlier Leopard releases had another problem where things were blocked on the second strike. I believe that has been fixed by now (10.5.3).

Adaptive Firewall

- To set up the whitelist and choose an interval for the blacklist entry aging (as root)

  /usr/libexec/afctl -c -i 10

- To add 69.23.0.45 to the blacklist for at least 35 minutes

  /usr/libexec/afctl -a 69.23.0.45 -t 35

Adaptive Firewall

- To add the address 17.254.3.183 to the whitelist so it will never be blocked by afctl

  /usr/libexec/afctl -w 17.254.3.183

- To make sure that the blacklist is preserved across reboots be sure to edit the startup_behavior key in the af.plist config file.
- http://developer.apple.com/documentation/Darwin/Reference/ManPages/man8/afctl.8.html

Adaptive Firewall Files

- Preferences
  - /etc/af.plist
- Whitelist - addresses that will not be blocked
  - /var/db/af/whitelist
- Blacklist - addresses that will always be blocked
  - /var/db/af/blacklist

Adaptive Firewall Files

- The launchd plist:
  - /System/Library/LaunchDaemons/com.apple.afctl.plist
- Don't edit the whitelist and blacklist files by hand - use afctl to manipulate them

Troubleshooting

- Firewall service requires planning and documentation beforehand.
- Make one change at a time and test that it did what you thought it would.
- If there are several admins who can make changes, make sure that all keep the shared documentation source up to date!

Troubleshooting

- If the rules look like they're working, but odd behavior is being exhibited
  (and time is less of an issue than determining problem)
- Use a packet sniffer
  - tcpdump is built-in

Troubleshooting

- To dump all packets passing through the en0 interface to the screen (stdout)
- tcpdump -i en0
  - For full protocol decode : tcpdump -i -vv en0
- Press ctrl-c to stop the capture
- Each line has time packet was received, protocol, source of packet, destination, and any other optionally set flags.

Troubleshooting

- Limit tcpdump to specific ports to narrow down problems
- Expand tcpdump to larger bytes of each packet with the -s switch (-s0 indicates unlimited size) and write it to file with the -w switch
  - tcpdump -i en0 -s0 -w server_trace.pcap

Troubleshooting

- Use the not command to exclude specific ports (ie ssh if you're ssh'd in)
  - tcpdump -i en0 host 192.168.1.45 not port 22
- For deeper analysis, write the dumps to a file and analyze them with more robust programs like Wireshark
- On the server side, just looking to see if the traffic made it through

Troubleshooting

- On the client side, looking for more in-depth details
  - Perform a half and half search
    - Disable half the rules
      - Is it broken? -No
    - Disable the other half
      - Is it broken? -Yes
    - And so on....

Troubleshooting

- Worst case - backup all the firewalls and flush
- Re-add half at a time
- When working remotely, don't forget to enable a "deadman switch"

Troubleshooting

- Just in case a rule is accidentally enabled that say stops SSH
  - Either an alternate route through another interface
  - or something like
    - sleep 90; sudo serveradmin stop ipfilter
  - which waits 90 seconds, and then completely stops ipfw (just in case)

Application Firewall

- ONLY available in Standard and Workgroup - not Advanced
- GUI via System Preferences > Firewall

Application Firewall

- To control connections based on applications (socket level) instead of per port/protocol
- Easy way to manage (aimed more at client than server)
- When in doubt - ipfw wins

Application Firewall

Application Firewall

- Works a level above and blocks traffic based on the target application (socket), not port.
- The top section of the window lists any running network services.
- These are automatically set when you start services on in the Sharing preferences pane, and you can't disable them from the firewall.

Application Firewall

- The firewall doesn't block any outgoing connections, something we'll discuss in a moment.
- For example, if you share iTunes at home, you can change the setting and manually block anyone from connecting when you're on a public network.

Application Firewall

- The application firewall also only blocks inbound connections; an attacker (or careless user) can still connect to hostile services and be compromised.
- An example was the Quicktime rtsp vulnerability in which an attacker could embed a link in e-mail or a web page, direct you to a hostile site in order to exploit your computer.

Application Firewall

- Had Apple included outbound blocking, you could have blocked Quicktime from network connections but still safely played files locally.

Command Line

- /usr/libexec/ApplicationFirewall/socketfilterfw
  - for managing rule sets
- defaults write /Library/Preferences/com.apple.alf globalstate -int 1
  - 0 = Off
  - 1 = On for specific Services
  - 2 = On for essential services

Application Firewall Locations

- Logs to /var/log/alf.log
- The editing application
  - /usr/libexec/ApplicationFirewall/socketfilterfw
- Main preference file
  - /Library/Preferences/com.apple.alf.plist
- Executable files
  - /usr/libexec/ApplicationFirewall

Application Firewall Locations

- http://developer.apple.com/documentation/Darwin/Reference/ManPages/man5/af.plist.5.html

For more information:

- OS X Server Manual
  - images.apple.com/server/macosx/docs/Network_Services_Admin_v10.5_2nd_Ed.pdf
- Mac OS X Advanced System Administration v10.5, by Edward R Marczak
- support.apple.com/kb/HT1810
  - only valid with X.5.1 and later
- from www.faqs.org/faqs/firewalls-faq/

For more information:

- docs.info.apple.com/article.html?path=ServerAdmin/10.5/en/c4ns15.html
- www.wikipedia.org
- www.afp548.com
- www.google.com

Contact Info

- Sara Porter
  - sarajgoo@mac.com
- Mike Sebastian
  - msebastian@powerofmac.com
- Slides:
  - www.powerofmac.com or .mac - msebastian

Thanks!