



Mercurion Systems, Inc.

Information Technology Consulting and Support Services

Phone: 919.266.5957 Fax: 919.217.5769
<http://www.mercurionsystems.com>

FIREWALL RULES FOR RENDEZVOUS

Products: Mac OS X 10.3 "Panther"

Overview

Apple's Rendezvous auto-discovery service (now called OpenTalk) is used extensively in many Apple-branded products, both hardware and software. For example, Mac OS X uses Rendezvous to advertise and discover iTunes music libraries. Apple's Airport Admin Utility also uses Rendezvous to discover Airport, Airport Extreme, and Airport Express wireless base stations for configuration. Multicast DNS (known as mDNS), part of the IETF standard known as Zeroconf, is used to provide this functionality.

Unfortunately, Mac OS X's built-in firewall, ipfw, does not have any GUI for allowing mDNS traffic; thus, Rendezvous doesn't work when the firewall is enabled. This technical note describes some firewall rules that can be added to the ipfw rules to allow mDNS traffic. With these rules in place, Mac OS X gains the benefit of added security through firewall protection while still benefiting from Rendezvous' auto-discovery features.

More Information

These rules were added to the ipfw configuration using Brian Hill's BrickHouse utility in Expert Mode (Quick Mode does not allow for the correct rules to be defined to allow mDNS traffic). Note that it is also possible, of course, to use the ipfw command directly within the Mac OS X Terminal application to add these rules.

Multicast DNS operates over UDP (IP protocol 17) port 5353. The destination address is, of course, a multicast address (in the 224.0.0.0 range). Responses to mDNS multicasts originate from UDP port 5353, but are bound for a random high port above 1024. Simply defining a rule that allows traffic to and from UDP port 5353 won't work, because while outbound traffic will be correctly matched the responses to those outbound requests won't be matched and will be dropped (assuming the default action is to deny traffic).

So, a sample rule to be added to ipfw might look something like this:

```
add 2008 allow udp from 10.1.1.0/24 5353 to any 1024-65535 in via en0
```

This rule allows traffic from the source network 10.1.1.0 (the "/24" indicating a 24-bit mask, i.e., a subnet mask of 255.255.255.0) from UDP source port 5353 to any port above 1024 on any destination address inbound via the en0 interface. The en0 interface is typically the built-in Ethernet interface on most Mac OS X-based systems.

To allow mDNS from other source networks, or on other network interfaces (for example, maybe on the built-in Airport/Airport Extreme wireless interface available on many Mac OS X-based PowerBooks or iBooks), additional rules can be added as illustrated below. (Note that allowing mDNS on the Airport/Airport Extreme interface is necessary for auto-discovery of base stations via Apple's Airport Admin Utility.)

```
add 5008 allow udp from 10.1.1.0/24 5353 to any 1024-65535 in via en1
add 5009 allow udp from 172.16.1.0/24 5353 to any 1024-65535 in via en1
```

Of course, these rules only allow for mDNS-based discovery; additional rules are needed to allow traffic to/from services discovered in this way. For example, these rules would allow for the discovery of a shared iTunes library, but actually accessing or using the shared iTunes library would require rules for daap (TCP and UDP port 3689). Similarly, accessing an SSH server discovered by Rendezvous (perhaps using the Apple's POSIX mDNSResponder running on Linux) would require firewall rules for TCP port 22 (SSH).

Other Notes

This document was specifically tested on version 10.3.5 of Mac OS X "Panther." In theory, however, the ipfw rules listed in this document should work on any version of Mac OS X that supports ipfw.

Related Articles/Resources

None

Legal Information

This document was created by Mercurion Systems, Inc., and may be freely distributed as long as it is distributed without modification and in its entirety. Mercurion Systems assumes no liability as a result of using the information contained in this document.