Making Apple Push Notification Service Available On Your Network

The Apple Push Notification Service (APNs) forwards notifications between MDM solutions to Apple iOS and OS X devices. The device makes an accredited and encrypted IP connection with the APNs, receiving notifications over this persistent connection via APNs.

APNs is a critical part of configuring and securing mobile devices. If there are things that prevent the direct and persistent connection to and from APNs then the entire MDM management capabilities will be inoperative.

APNs Networking Considerations

When Clients and MDM servers are behind a firewall, some network configuration may need to take place in order for the MDM server and device communication to function properly.

- Outbound traffic rules will allow the MDM server and clients to establish communication outbound from the host network, but will not allow traffic outside the host network to establish inbound communication to the MDM server, or clients.

- All communication will be established outbound, and should be allowed to bypass content filters, proxies, and firewalls to communicate directly with APNs.

- Though the communication is established outbound from the MDM server and from client devices, once connected to the APNs service, bi-directional communication will flow via that connection between the MDM server, clients and Apple.

- APNs uses a load balancing scheme that prevents static whitelisting of IP/port. As the entire 17.0.0.0/8 address block is assigned to Apple, firewall rules can be established to specify that range.

Clients and MDM servers require a direct connection to Apple's Push Notification Service (APNs).

A proxy server on the Wi-Fi network will prevent devices from being able to use APNs, because APNs requires a direct and persistent connection. Therefore, you will need to make the indicated ports open on your proxy server to guarantee the connection to APNs.

Some educational institutions that use ISP Co-Ops may have additional filters and should be provided this documentation.

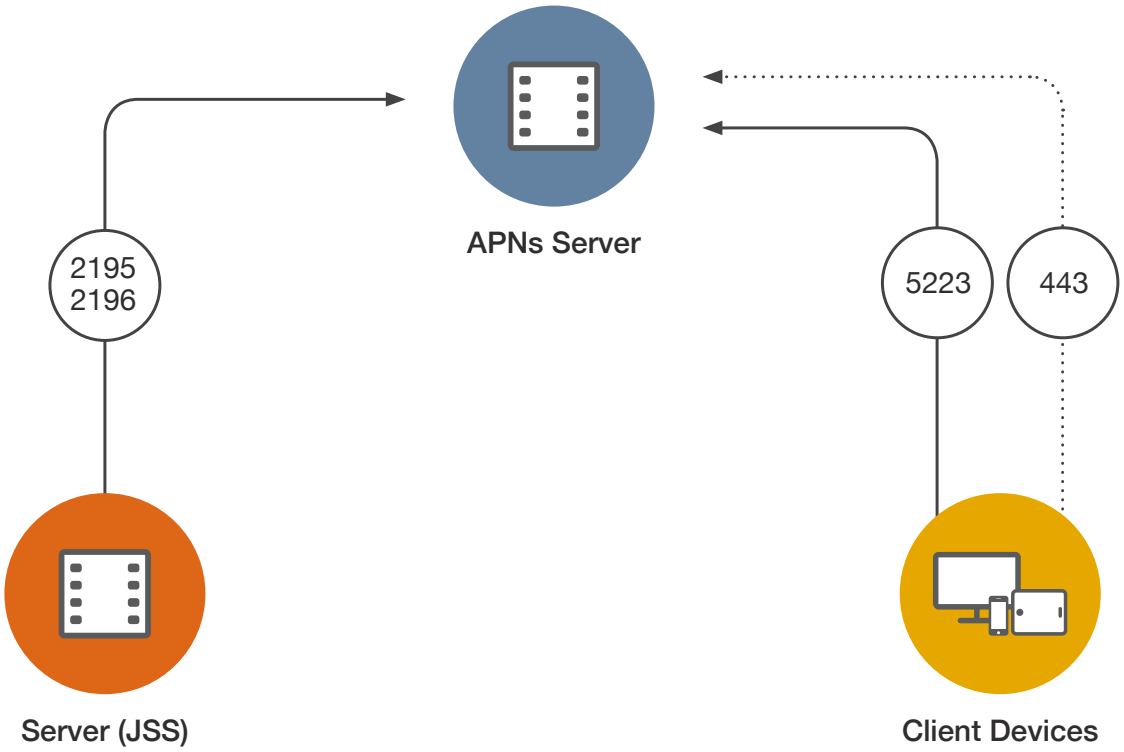
Clients

To ensure reliable client side communication, allow outbound connections to Apple's 17.0.0.0/8 block, over TCP port 5223, and 443.

MDM Server

To ensure reliable server communication, allow outbound connections to Apple's 17.0.0.0/8 block over TCP port 2195 and 2196.

Port	Description	Direction
443	Used as a fallback on Wi-fi only, when devices are unable to communicate to APNs on port 5223.	Outbound from computers and mobile devices to the APNs Server.
2195	The port used to send messages from the JSS to APNs.	Outbound from the JSS to the APNs Server.
2196	The port used by the JSS to connect to APNs for feedback.	Outbound from the JSS to the APNs Server.
5223	The port used to send messages from APNs to the iOS mobile devices and computers in your network.	Outbound from computers and iOS mobile devices, and inbound to the APNs server.



For additional information about APNs please consult the following Apple documentation:

https://developer.apple.com/library/ios/documentation/NetworkingInternet/Conceptual/RemoteNotificationsPG/Chapters/ApplePushService.html

https://support.apple.com/en-us/HT203609

JAMF software