Secure Mac network services

Setting up centralized servers allows you to take advantage of groups, policies and other traditional methods to protect file access on the network.

Network administrator - Mac, with outstanding advantages built on UNIX, is a more secure system than Windows. A lot of viruses, spyware, malware and "disease" network vulnerabilities for Windows computers are impotent against the Mac, but that doesn't mean the Mac doesn't interfere with these threats. . Here are some ways to protect your Mac from within corporate environments.

Secure file sharing

Very few network services are enabled by default on Macs. Automated services are usually required for network connectivity. That means that Mac systems respond to a small number of requests from external computers, which helps it increase security.
When enterprise administrators deploy Macs, files need to be shared from some centralized server. Setting up centralized servers allows you to take advantage of groups, policies and other traditional methods to protect file access in a secure network.

In cases where files need to be shared from individual Macs, whether using AFP, FTP or SMB, you need to configure the systems to require user authentication. Anonymous FTP is disabled on Macs by default; You should not reverse this setting. In addition, guest access should also be disabled from within the Account

preferences.

Remember, when file sharing is enabled, administrative users can remotely *mount* (mount) any partition or drive and both administrative and standard users can access the folder at their home remotely. Public folders are automatically shared when new administrative or standard users are added.

Unless there is a reason for some extra theory, business administrators should disable these default settings within the **Sharing preferences** or **Finder** 's **Get Info** window to increase security. Customize file sharing through the **Finder** window within its **Sharing & Permissions area** , allowing additional tweaking of any file sharing enabled on the Mac.

Secure screen sharing

Macs include screen sharing features designed to assist in troubleshooting remote clients. This feature uses an encryption form of the Virtual Network Computing (VNC) protocol. Because the feature will enable viewing and remote control of the Mac, you need to be careful to ensure network security. The service, when enabled within the System Preferences Sharing interface, will listen for UDP and TCP traffic on port 5900.

When screen sharing is enabled, or when enterprise administrators buy Apple Remote Desktop (ARD) remote registration, the service will be activated. By default, all non-guest users are allowed to access the service. Therefore it is best to limit sharing terms, then only allow on systems where this feature is required (it should be disabled on systems where possible to tighten security issue). When the service needs to be activated, the administrator needs to specify which users will be allowed to access the screen sharing feature.

Within the Screen Sharing interface, select the **Allow Access For** button to restrict screen sharing access to some users on your list. List which user accounts to authenticate can perform support and remote management activities.

Mac firewall

Many enterprise administrators deploy solid firewalls in the network perimeter. However, hardware routers that protect internal networks are not very easy to use. When the first step is required, they only protect the systems on the other side of the wall at a moderate level, nor do they protect the client system gateway firewall when the system works outside by employees. mobile. That is why enterprise administrators should consider promoting the advantages of Mac application firewalls.

Mac OS X's personal application firewall Snow Leopard can take advantage of rules and enable / disable traffic 'dynamics' to better protect network services. It allows network connections based on service and application requirements, not just static ports, so better protection of mobile systems compared to hardware devices is not always present. . Because the firewall is active, it will improve security.

Consider adding an IM program. When the user logs in and iChat is opened, the individual application firewall will allow the necessary ports for the application's operation. However, when they close the application (or other services, when logging out), the Mac firewall will close those ports, so it will tighten security issues.

The Mac firewall is activated from within the System Preferences Security interface. Click the **Firewall** tab to open the firewall interface. Logging is always enabled. The recorded information will be stored inside the file /private/var/log/appfirewall.log. In addition, the firewall can be customized. Using the **Advanced** button, you can check the positive services and adjust certain services.

You finished reading the article "**Secure Mac network services**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
