Product Comparison

Proxy Networks Private Cloud Edition vs Windows RDP

PROXY Networks

Proxy Networks, Inc.
320 Congress Street, 3rd FloorBoston, MA 02210
1-877-PROXY-US / 1-877-776-9987

Key Features	Description	RDP	PROXY Pro Private Cloud Edition
Internal Connectivity	Connect and support machines within your LAN	Yes	Yes
External Connectivity	Connect and support machines outside your LAN	No	Yes
File Transfer	Transfer individual files or entire directories	No	Yes
Chat	Open a chat window between you and the end user	No	Yes
Screen Recording/Playback	Record a session and play it back	No	Yes
Centralized Directory of Machines	View a persistent list of all machines, both online and offline	No	Yes
Real-time Screen Sharing	View and remote control end users' machines, allowing the technician to see the same screen as that of the end user	No	Yes
Many-to-One Connectivity	Multiple technicians may simultaneously connect to end users' desktops	No	Yes
Customizable Access Rules	Create separate access rules for Tier 1, Tier 2 and Tier 3 helpdesk teams	No	Yes
Centralized Auditing of Connections	Generate activity reports reflecting all connections made either by technician, or by connections made to specific machines	No	Yes
256-bit Encryption	Fully encrypted data stream for all connections	No	Yes
"Stealth Mode" Connections	Connect silently without any indication to the end user	No	Yes
Require End-User Permission	End users receive prompt to allow or reject a connection attempt	No	Yes
Centralized Database	Persistent database all desktops, laptops or servers, on or off	No	Yes
Wake-on-LAN	Wake a machine in a reduced power state and connect	No	Yes

Additional information on the next page...

What specific RDP-related challenges can be alleviated with a Proxy Networks solution?

1. RDP is technically not a true remote support tool because when a Support Team member establishes a connection to an end user's computer via RDP, the end user's Windows session becomes locked as it is now in use by the technician who connected.

2. When supporting end users, you may need to transfer files to their machine and this is not available in RDP but is included in every version of Proxy.

3. The process to connect to a machine with RDP is to open the Remote Desktop client and then enter the target computer's IP or computer name, requiring you to either know this information in advance, or ask the end user for one of those two things, potentially requiring some level of end-user intervention. The moment you open the Proxy Master, a complete listing of all available Proxy Host machines appear immediately and to connect to a user named "John Smith", simply look for it on the list and double-click to connect.

4. One of the common requirements (depending on industry) we hear is that end users must explicitly "Allow" a connection to occur. RDP has no such mechanism and Proxy does (in more than one fashion to boot). The Proxy Host can be configured such that when a member of your IT Support Staff attempts to connect, end user approval is required, but when a Domain Administrator attempts to connect, they connect immediately and bypass the connection permission prompt which is ideal for maintenance or for emergency situations.

5. Especially in larger networks with multiple helpdesk personnel, one team may be responsible for supporting only a sub-set of all of the machines in your network. The Proxy Host allows you to create a list of who, by AD accounts or groups, has the ability to connect. Furthermore, because Proxy includes many additional pieces of functionality over RDP, you can do more than defining who can connect. For example, you can enable or disable File Transfer, the ability to start Chat sessions, the ability to copy/paste clipboard content back and forth, and you can even dictate that certain users can only connect in "View-Only" mode and not actually take control of the end user's keyboard and mouse if you so choose.

6. All connections made with Proxy Networks software are fully encrypted by default - we use AES encryption (256-bit key) with SHA1 hash over our proprietary data stream, dating back as far as 1993.

7. There have been numerous security-related issues with Windows RDP that Microsoft continually needs to patch once new exploits are discovered by malicious parties. Although Microsoft has always been very diligent about fixing and resolving security vulnerabilities that are discovered in and around RDP, here are a few articles that go into more detail:
    - http://technet.microsoft.com/en-us/security/bulletin/ms12-020
    - http://www.scmagazine.com/microsoft-patches-ie-rdp-security-vulnerabilities/article/245433/
    - http://en.wikipedia.org/wiki/Remote_Desktop_Protocol#Security_issues
    - http://support.microsoft.com/kb/2508062
    - http://support.microsoft.com/kb/899591

Although there are more articles that can be found on the internet relating to RDP's history of security issues, Proxy's secure, proprietary, always-encrypted data stream has never had a history of issues like this.

Furthermore, one of the most important benefits of Proxy Networks Private Cloud Edition is that connections can be made quickly and easily by performing a "Host Search", where a technician enters either the target machine's computer name, or the identity of the user you are trying to support.

Proxy Networks, Inc.
320 Congress Street, 3rd FloorBoston, MA 02210
1-877-PROXY-US / 1-877-776-9987