PROXY Networks

SECURITY WHITEPAPER:

7 “Must-haves” to Ensure Remote Access Security across your Organization

INTRODUCTION

There are a multitude of remote desktop software tools in the marketplace today that enable IT and support professionals to provide remote access, remote control and remote management to computers, laptops, systems and servers across the enterprise. Now, while there is a wide range of functional capabilities in these solutions, there is an even larger gap in degrees to which those solutions are an asset to your company's security requirements, versus those that put your enterprise at risk.

This whitepaper focuses on the information security components of remote desktop software that your organization must consider to ensure remote access security across your enterprise.

7 SECURITY "MUST-HAVES"

1. Authentication… *"Show me some ID, please"*

Strong Windows Authentication is the foundation for security, and in most organizations this is done using the Windows Security Model. This allows you to define all security and create a policy tied to your pre-existing Users and Groups within your Active Directory domain, and then requires users to provide the proper credentials.

In accordance with Windows Security, you can then confidently support Windows Single Sign-On, based on authorized users of the software. Users that are already logged into Windows can be automatically logged in to your remote desktop software, assuming they are logged into Windows as themselves, because the software will typically support the authentication via this existing Windows user account, as defined in A.D.

The same principles hold true for lock-out policies, if enabled. And in the event that a user leaves your company, simply disabling the account in A.D. (or changing the password) will lock this user account out, preventing their ability to authenticate entirely.

2. Authorization… *"Sorry, but I don't see you on the list."*

It is critical to have an authorization model built right into your software, whereby you can explicitly grant specific users the authority to access remote machines. Furthermore, you should be capable of defining, at a very granular level, what groups of desktops they can view and connect to, and what specific pieces of the remote desktop software's functionality are available to that user. For example, you may decide that junior level users are not authorized to perform file transfers, or remote administration tasks, or initiate screen recordings. Authorization security is ideal in multi-tiered helpdesk environments, for allowing outside contractors remote access, or for segmenting responsibility to different groups of desktops.

3. End-User Permission to Connect… *“May I please come in?”*

Each organization must design its own policy with regards to attended and unattended remote access, and determine whether end-user permission should be required. Permission to connect can add a layer of security (or courtesy) if your business processes support that, and should be easily configurable within your remote desktop software solution. Other considerations may be some of the following:

- **No Permission Required** - Connections will be made without end-user intervention (the default)

- **Permission must be granted** - Connections will only be made after an end-user explicitly allows the connection, and the connection will be rejected if the user does not allow it within the specified timeframe (10, 30, 60 or 120 seconds).

- **Permission requested from end-user, but access granted if no response -** This option gives the end user the courtesy of allowing the connection, but will allow you to connect to the machine if there is no response from the end user within the specified timeframe. Additionally, if there's no response, you may want the software to lock the workstation so that logging into Windows is required to begin using the machine again.

4. Encryption… *“Now you read it, now you don’t.”*

There have been numerous reports of data in transit being intercepted in recent years, thus encryption (and decryption) will lessen your risk for data security vulnerabilities. In addition, Encryption and Decryption are key requirements for PCI DSS and HIPAA compliance specifications.

You should ensure that all connections made with your remote control software are using AES encryption (256-bit key) with the SHA1, by default.

5. SSL Protocol… *“Do you know the secret handshake?”*

SSL protocol allows client-server applications to communicate across a network in a way designed to prevent eavesdropping and tampering. Although all connections should be fully encrypted over UDP and TCP, the key value-add of SSL over encrypted TCP is the SSL certificate, which guarantees that it is talking to the right server or gateway. If you require that all available security avenues be pursued, this can further help you ensure that your data is kept secure.

6. IP Address Restrictions… *"On the road to nowhere"*

If you security policies require greater degrees of mitigation against potential brute force attacks from malicious parties, you might consider implementing IP address restrictions for remote control connections. That way, your software should either "Allow All Except..." or a "Deny All Except" connection attempts that originate from a definable IP address range.

7. Real-Time Auditing… *"Who, when, what, and for how long."*

The final "pillar" of remote access security is the ability to have real-time assurance that your security strategy works! That can only be done with through robust reporting and analytic tools that audit all attempted remote connections (whether successful or failed), and all remote "services" preformed in those remote control sessions.

Auditing is now the standard for accountability and often a key requirement for internal and external compliance. And if you have gone through all the trouble to develop and implement a remote access policy at your organization, you'd better well be able to back this up with an audit trail.

GET A FREE SECURITY ASSESSMENT TODAY!

To learn more about our Remote Desktop Software and Security, please contact our team at:

Email:	info@proxynetworks.com
Web:	www.proxynetworks.com
Phone:	**877.776.9967**

> **"As a PROXY user for over a decade, I have always been a strong advocate for their remote desktop software. With our move to the PROXY Private Cloud Edition, I am happy to say that we can eliminate the use of any additional remote access tools across our entire IT organization"**
>
> Sheila A. Setser
> Chief Systems Engineer
> Scott County Public Schools