Extending Your Management Reach to Remote Users

LANDesk®

White Paper

Table of Contents

Executive Summary 3
Obstacles to Cost-Effective Remote Management 3
Problematic Solutions 3
A Meeting Place to Bridge the Gap 4
Tools for Offense and Defense 4
Extending the Defensive Perimeter 5
Is LANDesk® Management Gateway Secure? 6
Are Firewall Changes Required? 6
Conclusion 6

This document contains confidential and proprietary information of LANDesk Software ("LANDesk") and its affiliates and is provided in connection with the identified LANDesk product(s). No part of this document may be disclosed or copied without the prior written consent of LANDesk. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in LANDesk's terms and conditions of sale for such products, LANDesk assumes no liability whatsoever, and LANDesk disclaims any express or implied warranty, relating to sale and/or use of LANDesk products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. LANDesk products are not intended for use in medical, life saving, or life sustaining applications. LANDesk does not warrant that this material is error-free, and LANDesk reserves the right to update, correct, or modify this material, including any specifications and product descriptions, at any time, without notice.

LSI-0434 0905 JBB/JA

Executive Summary

Without question, “anytime, anywhere” access to corporate resources is more of a business imperative today than ever before. Mobile workers increasingly consider the privilege of remote access an “inalienable right” on par with “life, liberty, and the pursuit of happiness.”

But with the increasing demands for far-flung connectivity come new threats to network and systems security, and the ever present pressures on IT professionals to manage these remote computing endpoints as though they were within the corporate network.

This whitepaper examines how the LANDesk® Management Gateway in LANDesk® management solutions 8.6, along with LANDesk® Trusted Access™, help organizations extend the enterprise management of remote devices across the Internet without having to “punch holes” in the firewall or compromise the security of such devices or the corporate infrastructure.

Obstacles to Cost-Effective Remote Management

In the past, organizations with employees that work outside the corporate firewall have found it extremely difficult or expensive to manage these workers’ computers. To be able to provide remote users the same level of support enjoyed by users within the corporate boundaries would typically require dedicated leased lines or VPN solutions. But since these workers at remote locations are frequently few in number or even temporary in nature, it’s often a leap to justify the cost of such connectivity.

Consider these IT support scenarios for example:

- Remote sales offices, typically staffed by a few workers in each office
- A home builder who relocates a mobile office to a subdivision for the duration of the construction project
- A proposal writing consultant team that works onsite at a defense contractor for two months
- Franchised restaurants that upload financials, place orders, and download corporate data
- An IT task force that travels abroad for three weeks to resolve obstacles to a new software implementation
- An emergency response unit of a government agency that sets up operations in a disaster area
- A jewelry manufacturer that opens a series of kiosks in shopping malls, each staffed by one or two people

Problematic Solutions

Some organizations turn to dial-up connections only to battle with an array of problems that result from slow speeds, low bandwidth, and the lack of a dedicated connection. Software distribution and patch deployment take too much time. Real-time device monitoring, scanning, and inventorying become problematic or near impossible. Remote troubleshooting of users’ computers is slow, cumbersome and typically requires considerable user involvement, all leading to higher support costs and significant productivity losses.

Instead of using leased lines or dial-up connections to apply patches or distribute software updates to remote users, some organizations create distribution CDs at their corporate headquarters and then mail them to the remote sites in hopes that they’ll be deployed once they arrive. To ensure that the CD does get deployed, they’ll often fly out an engineer with the CD to the site or hire a local contractor to implement the deployment.

Regardless of the option they choose, these methods delay vulnerability remediation, breed inconsistency in security policy compliance, hinder productivity, and lead to higher support costs. Furthermore, these practices do not address the issue of how to track and manage remote inventory and asset information.

Realizing the ineffectiveness or high costs of these different remote management schemes, some organizations instead leverage the ubiquitous and inexpensive connectivity offered by the Internet. However, this typically has required them to “punch holes” in their corporate firewalls, thereby opening the door to intruders and malicious attacks on their enterprise infrastructure.

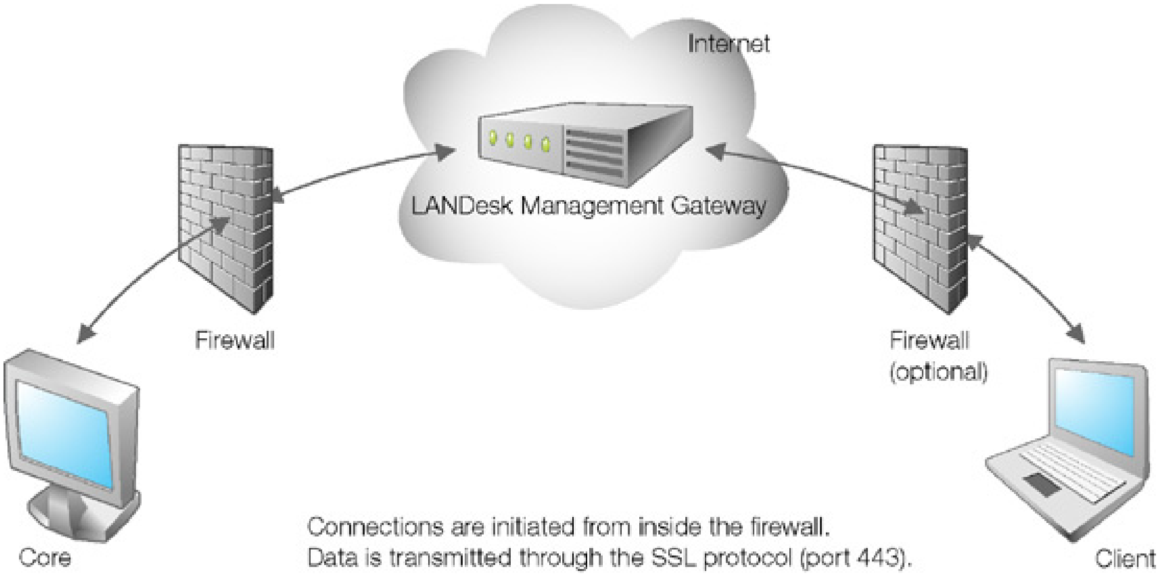
A Meeting Place to Bridge the Gap

The LANDesk® Management Gateway in LANDesk® management solutions 8.6 lets you manage devices not connected to the local network, without the need to punch holes in the firewall. This solution using patented technology enables organizations to improve business processes, protect corporate data and comply with regulatory requirements through comprehensive endpoint security and configuration management tools. It allows organizations to:

- Protect corporate data and improve business process efficiency with comprehensive security and configuration management in a single, unified solution
- Demonstrate compliance to standards and regulations across complex, heterogeneous computing environments with comprehensive asset management and configuration control reporting
- Protect corporate computing assets from malicious attacks with security policy evaluation and enforcement
- Maintain centralized management control through both direct connections over corporate networks, and remote connections over the Internet

The LANDesk Management Gateway acts as a meeting place where the core console and managed devices are linked through their Internet connections—even if they are behind firewalls or use a proxy to access the Internet.

Using a secure SSL tunnel, the LANDesk Management Gateway continuously routes bi-directional data between the two computers as long as they are connected. The SSL data is not decrypted at the LANDesk Management Gateway, so there is no “hole” in the protocol where the data isn’t encrypted. This provides security, allows a larger number of connections by minimizing CPU utilization, and eliminates the need for complex synchronization between the connections—when data is received, it is sent on to its destination without delay.


Internet
LANDesk Management Gateway
Firewall
Firewall
(optional)
Core
Client
Connections are initiated from inside the firewall.
Data is transmitted through the SSL protocol (port 443).

The LANDesk Management Gateway runs LDLinux, a customized version of the Linux 2.6.12 kernel. It uses standard messaging, Web, and database services. It also logs connection information (such as connection time, bytes transmitted, and identification information) to the server’s hard drive. The program itself uses minimal hard disk space; most disk space is used for logging purposes.

Tools for Offense and Defense

The sports maxim “the best defense is a good offense” also applies to endpoint security management. While organizations are increasingly more adept at blocking infected e-mails and preventing malware downloads before they can reach users’ computers, viruses and other malicious code often penetrate network security by hitching a ride on mobile computers that have journeyed beyond the perimeter protection of the corporate network. What’s more, any endpoint device within the network that is inadequately protected can become infected and unknowingly act as a malicious carrier.

The offensive capabilities of the LANDesk® Management Gateway are complemented by LANDesk® Trusted Access™—a new scan-and-block technology that not only blocks possibly infected computers from connecting to the network, but also allows for quick remediation of the offending machine. For the first time, customers can reach out to remote endpoint devices over the Internet and preempt threats before they ever get to the network.

In the case of a large soft drink distributor, for example, employees returning from a trip overseas brought back an unidentified virus on their laptops that spread to other machines on the network. With LANDesk Management Gateway and LANDesk Trusted Access, the distributor would have been able to scan the laptops over the Internet and remediate any vulnerabilities before connecting them to the corporate network. Then, if by chance any threat were missed, LANDesk Trusted Access would scan, block and quarantine them from the network.

With these new tools, laptops and other remote devices that were once considered unreachable can now be updated, fixed, scanned, inventoried, and monitored just as if they were on the corporate network.

Extending the Defensive Perimeter

LANDesk® Management Gateway and LANDesk® Trusted Access™ make it easy to extend the defensive security management capabilities of LANDesk® Security Suite to remote users, including centralized patch management, connection control configuration, anti-spyware, configuration security threat analysis, application blocking and anti-virus enforcement.

Whether your endpoint devices reside remotely or within your corporate network, LANDesk Trusted Access enables you to:

- Prevent infected or unprotected systems from gaining network access
- Protect corporate resources from connected systems that become corrupted
- Set compliance standards
- Enforce security policies that endpoint devices must meet before being passed onto the corporate network

By taking advantage of the LANDesk Management Gateway, you can employ secure systems management across the Internet using the following features inherent to LANDesk Management Suite 8.6 and other LANDesk management solutions:

- Inventory gathering
  - Hardware
  - Software
- Software license monitoring
- On Demand remote control features
  - Remote keyboard, video and mouse control
  - File transfer
  - Chat
  - Remote execute
  - Screen draw
  - Reboot
- Policy-based software distribution
- Security functions (via LANDesk Security Suite and/or LANDesk® Patch Manager)
  - Patch management
  - Custom definitions for patch management of any application(s)
  - Anti-spyware management
  - Security threats
  - Blocked applications
  - LANDesk updates
  - Connection control
  - Anti-Virus enforcement

Is LANDesk® Management Gateway Secure?

Connections through the LANDesk® Management Gateway make use of digital certificates and a novel, dual-SSL session architecture. Sessions are initiated by the managed device, which first communicates with the LANDesk Management Gateway itself. The second SSL session encloses the entire route, end-to-end, allowing data to be transferred between the managed device and console computers. This second SSL session eliminates the need for the LANDesk Management Gateway to do any decrypting or re-encrypting of data. This increases session security and reduces the resource load on the LANDesk Management Gateway itself. Data is decrypted only when it arrives at the destination.

Are Firewall Changes Required?

If your firewall is set up to allow secure Internet transactions using port 443 and SSL, using the LANDesk® Management Gateway will not make any changes in your firewall, nor will it change how your firewall behaves. The LANDesk Management Gateway uses standard protocols to work through firewalls, proxies, and NAT routers, without requiring any infrastructure changes and without opening any ports.

Conclusion

The LANDesk® Management Gateway delivers anytime and anywhere systems management. As long as remote computers have a connection to the Internet, they can now be managed and secured as easily if they existed inside the corporate firewall, resulting in comprehensive management of all systems, faster problem resolution, less downtime, increased end-user satisfaction, improved productivity, and significantly lower support costs.