

Solution Brief

Provisioning for Today's Thin Client Computing Environments with Secure Access SSL VPN

Overview

Thin client computing (TCC), otherwise known as server-based computing, was designed to drive down the high costs associated with running applications on every desk top, enabling access to applications written for one computing platform from other platforms, and providing remote access/control of applications. Companies like Citrix, have created entire businesses based on offering this technology. Nonetheless, IT departments are constantly struggling with the costs associated with managing and securing TCC environments as the number of users and applications grow. The escalating demands have often forced IT departments to establish monthly budgets for the sole purpose of adding new TCC resources, like additional Citrix end user and server licenses.

Situation

TCC is becoming increasingly competitive and the technology continues to evolve. With many of the advancements in Microsoft Terminal Services (MSTS), companies are beginning to re-evaluate the number of applications that depend on the TCC services, like Citrix. New advancements and features are giving IT departments more flexibility by facilitating use of the best and lowest cost TCC technology products, which can result in significant capital expenditure and operational cost savings.

For example, Citrix deployments are required to run on top of Microsoft Terminal Services deployments. Companies who have installed Citrix must have Microsoft Terminal Services deployed. By provisioning some applications and users from Citrix to Microsoft, companies are able to cost effectively use Citrix for only selected applications really requiring its selective usage or provisioning completely to other product offerings with add-on functionality to MSTS. By eliminating the number of users on Citrix, IT can re-allocate large existing budgets set aside for additional Citrix users licenses to other priorities.

Customer Value

SSL VPNs have always been used as a natural extension of TCC to

- Provide remote access to corporate resources
- Provide the ability to authenticate, authorize and audit thin client traffic
- Ensure end point device defense
- Control access based on the combination of user, end point device and network information
- Enable granular control of remote application access

The advent of more and more IT departments provisioning their applications from Citrix to Microsoft Terminal Services has made it essential that any secure remote access deployment can provide the same security for both solutions. The strength of Juniper Networks Secure Access SSL VPN is that one Secure Access appliance can provide the security required for protecting both Citrix and Microsoft Terminal Services environments equally, without sacrificing the full feature support of one TCC application over another. TCC vendors often offer SSL VPN as extensions to their product. While they often provide adequate SSL VPN functionality for their proprietary environment, they often inadequately provide SSL VPN functionality for other applications.

Citrix and Microsoft Terminal Services are only two of several thin client computing applications in which Secure Access provides extended access capabilities. Companies such as, Ericom, Provision Networks, HOB and more can provide the added functionality currently lacking natively on MSTS, such as load balancing, true seamless windows, and better application provisioning using Microsoft's Remote Desktop Protocol (RDP), as opposed to Citrix's ICA Protocol. The strength of Juniper Networks Secure Access SSL VPN is that it provides the richest functionality for providing secure remote access for all thin client computing environments in the same manner, regardless of the underlying protocol used. Secure Access provides flexibility for any remote access deployment, enabling IT to make remote application access consistent for all users.

Conclusion

Many companies continue to take advantage of TCC to reduce overhead costs associated with higher cost applications. Juniper Networks Secure Access is complimentary to any TCC application. Secure Access provides remote access without client side software or hardware to email, applications, telnet/SSH, and file sharing.

New developments in TCC continue to give companies more flexibility in choosing the best and most cost effective solutions for their environments. In many cases, companies have started to provision their applications across multiple TCC environments to contain costs and open budgets for other critical resources. Juniper Networks Secure Access SSL VPN provides the most comprehensive support of all TCC environments to ensure the most secure access and transfer of data, to provide the best end point defense, to enable best in class granular control based on the user, end device and network, and to provide the best authentication, authorization and auditing for remote access of client server applications.



CORPORATE HEADQUARTERS
AND SALES HEADQUARTERS
FOR NORTH AND SOUTH AMERICA

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888-JUNIPER (888-586-4737)
or 408-745-2000
Fax: 408-745-2100
www.juniper.net

EAST COAST OFFICE
Juniper Networks, Inc.
10 Technology Park Drive
Westford, MA 01886-3146 USA
Phone: 978-589-5800
Fax: 978-589-0800

ASIA PACIFIC REGIONAL
SALES HEADQUARTERS
Juniper Networks (Hong Kong) Ltd.
Suite 2507-11, Asia Pacific Finance Tower
Citibank Plaza, 3 Garden Road
Central, Hong Kong
Phone: 852-2332-3636
Fax: 852-2574-7803

EUROPE, MIDDLE EAST, AFRICA
REGIONAL SALES HEADQUARTERS
Juniper Networks (UK) Limited
Juniper House
Guildford Road
Leatherhead
Surrey, KT22 9JH, U. K.
Phone: 44(0)-1372-385500
Fax: 44(0)-1372-385501