

SSL VPN: The Ideal Approach for Establishing Secure Access to Virtual Desktop Infrastructure Solutions

Sponsor: Juniper Networks

Author: Mark Bouchard

AimPoint Group
keeping IT on target

Introduction

Because of the many technical and business-oriented benefits it provides, virtual desktop infrastructure (VDI) appears well on its way to becoming a mainstream IT solution. Early adopters of this technology consistently confirm anticipated value propositions—including lower operating and desktop hardware costs, reduced risk of data loss, improved user productivity, and the ability to more readily adapt to changing business requirements. What organizations need to realize, however, is that maximizing these gains depends on establishing a means to secure remote access to computing resources delivered in this manner. For that matter, what users and IT administrators ultimately need is a single, consistent approach for enabling secure remote access to all of their organization's applications, services, and information resources—not just those served by VDI.

This paper identifies the benefits and challenges associated with virtual desktop infrastructure and explains why SSL VPN technology is an ideal approach for securing access to VDI environments. It also provides guidance on how to select the right SSL VPN solution for the job.

Understanding Virtual Desktop Infrastructure

Although VDI holds promise as a game-changing IT solution and, therefore, is expected to explode in popularity over the next five years, it is not without its challenges.

VDI Fundamentals

Traditional desktops are hard-coded combinations of OS, applications, data, and user settings all tied to a specific piece of hardware. In contrast, desktop virtualization is an approach that abstracts, or separates, the desktop workload from the client-computing device. Technically, VDI refers to the scenario where the desktop workload is contained in a virtual machine and run remotely on a server virtualization solution (for example, VMware vSphere) in the data center. For the purposes of this paper, however, this definition is expanded to encompass all server-side virtual desktop models—such as options where the desktop environment is run on server-based computing technology (i.e., terminal services) or blade PCs as well.

Other core components of leading VDI solutions, such as those from Citrix and VMware, include:

- **One or more management systems**—These are used to administer the individual elements of the desktop environment, compile and provision desktop images, and manage backend resources such as the server virtualization system and associated storage resources.
- **A connection broker**—This proxies remote requests for desktop services, enforces applicable policies, marshals the required VDI resources, and maps users to a corresponding desktop image.
- **A client component (i.e., agent) and display protocol (e.g., ICA for Citrix and RDP or PCoIP for VMware)**—These establish an isolated workspace on the client and handle the exchange of keyboard, mouse, and display updates, respectively.
- **Support for offline operation**—This capability enables users to “check out” an instance of their desktop environment and stream it to their client device where it can then be run locally.
- **Support for application virtualization**—This capability further extends the benefits of virtualization by also enabling separation of applications from the desktop image.

Why VDI Matters

The growing attraction to VDI is fueled by the vast array of benefits derived from its isolation capabilities and centralized model for implementing and managing desktops. To begin with, VDI helps address several technical problems that IT organizations have historically encountered with distributed desktops, such as:

- The deployment and maintenance headache that ensues from trying to keep up with new versions of operating systems, client software, bug fixes, and security patches
- The poor performance that results when client/server workloads are not properly designed for operation over the WAN
- The challenge of supporting a diverse set of client platforms and operating systems when applications were originally designed to only run on a given system and/or hardware configuration
- The challenge of adequately securing remote systems and efficiently backing up associated data

Alternately, considering matters from a business perspective, the benefits of VDI can be grouped into a handful of compelling categories.

Lower cost of ownership—Desktop operating costs are typically reduced by 50 percent or more compared to conventional deployment models. With VDI, not only are all elements of the desktop environment run and maintained centrally, but also they are isolated from each other—a characteristic that further streamlines management processes and virtually eliminates compatibility issues. Substantial savings can also be realized on the capital side of the ledger based on the ability to defer the purchase of new desktop systems and/or take advantage of thin-client platforms, repurposed thick-client PCs, and user-owned devices.

Greater productivity (for users and administrators)—Users receive better and more timely technical support due to the centralization of both administrative personnel and the software/systems on which they operate. Recovering from many types of client system failures requires nothing more than having affected users restart their session. And workforce continuity is virtually guaranteed during disasters and disruptions as VDI provides displaced users with a nearly universal solution for accessing the resources they need to get their jobs done. Productivity gains are also derived by the improvements to desktop stability and availability that result from having centralized control over desktop images, simplified compatibility testing, and the ease with which a centralized backup and recovery solution can be implemented.

Reduced risk—With VDI, sensitive data is kept in the data center, where it is typically protected by robust, centralized security infrastructure—as opposed to being located on relatively vulnerable client devices that are easy to lose. In addition, a smaller software footprint presents less surface area for attacks against client devices, and centralized control means that applicable patches and security countermeasures can be implemented more quickly and thoroughly.

Greater business agility—Changing business needs can be addressed in a matter of minutes as new desktops and applications can be provisioned and made available to anyone, operating in any location, with virtually any device. Furthermore, branch expansion projects, tactical or strategic partnerships, teleworking initiatives, and mergers and acquisitions can all be facilitated without having to establish costly computing infrastructure at each new location.

Given this extensive portfolio of benefits, it is not surprising that the VDI market is poised to take off. Indeed, estimates attributed to Gartner have the worldwide hosted virtual desktop market growing from 500,000 units and revenue of \$1.5 billion in 2009, to 49 million units and \$65.7 billion in 2013. And although these projections seem somewhat optimistic, it is not unrealistic to expect greater than 50% of all organizations to be using desktop virtualization in some capacity by 2011. After all, associated vendors also have the benefit of being in a position to build off of (a) the high degrees of success that organizations have previously experienced with both server virtualization and server-based computing technologies, and (b) the opportunity that the availability of Windows 7 represents for organizations to rethink their client-computing strategy.

VDI Challenges

VDI certainly has a lot to offer. Like any other technology solution, however, it is not without some issues and potential challenges. For instance, one of the most prolific trends facing modern organizations is the growing separation between users and the information resources they require to get their jobs done. At the same time that workers are being spread out all over the globe to support fast, flexible, and far-reaching business models, computing infrastructure is being centralized and consolidated to reduce costs, improve security, ease compliance efforts, and better ensure availability. Consequently, one of the key challenges pertaining to VDI is the need to establish a means to securely access hosted desktops remotely. At a minimum, users' identities must be verified, and the confidentiality and integrity of their sessions must be assured as they communicate over open/public networks.

Of course, the need to provide secure remote access is not the only challenge organizations face. Other factors that can complicate VDI implementations include inconsistent availability of the capability to work offline; difficulty handling certain types of applications (such as those involving intensive graphics or video); a lack of adequate visibility and/or support among common systems management tools; and the effort and complexity required to ensure the scalability, availability, and accessibility of associated server and storage infrastructure. Indeed, each of these potential issues reveals why VDI, despite its many strengths, is actually not appropriate for all use cases—a conclusion that applies even once it is in place as an available solution.

A simple example that reinforces this latter point involves a user operating from a kiosk in a hotel or an airport. Downloading a VDI client might not even be possible in this case due to rights restrictions. But neither would it be warranted if all the user wanted access to was something such as Outlook Web Access.

The key takeaway here is that the vast majority of organizations are unlikely—at least in the foreseeable future—to rely solely on VDI. Instead, VDI will be used alongside other conventional deployment techniques, enabling IT to deliver desktops and applications in the manner that is best suited for each of the use cases it's ultimately required to support.

Summarizing matters from the perspective of the IT department then, what we have is the following:

- VDI is an attractive model for desktop delivery and management that needs to be supported.
- This support needs to include a means for securely accessing virtual desktops from remote locations.
- Hosted virtual desktops are not universally applicable or appropriate and, therefore, are not the only resources to which users require access.
- Implementing several different solutions for secure remote access would be highly inefficient.

Then there is the users' perspective. What they really care about is having one consistent and reliable way to access all of the resources they need, whenever and wherever they need them.

Providing Secure Access for VDI Environments

The good news is that organizations have several options for enabling secure remote access to their VDI implementations. The bad news is that the different approaches vary considerably in terms of efficiency, breadth of capabilities, and overall degree of effectiveness.

The Typical Contenders

Conventional techniques and technologies include taking advantage of native security features, employing solution-specific security gateways, or implementing an IPSec VPN.

Native security features—Many VDI products include a handful of native security capabilities, often as integral features of their connection broker. These incur no added cost, but are often very basic. Typical in this case is support for basic user authentication, authorization to establish which desktops a user has access to, and the ability to encrypt session traffic (e.g., using SSL). Related limitations include that these features only work for resources provisioned with the given VDI product and that they are inherently part of the desktop/server infrastructure and, therefore, contribute to its complexity and the related challenges of scaling and managing this infrastructure.

Solution-specific security gateways—Some VDI products include optional, standalone gateways or other add-on feature sets that provide core services to secure access to the VDI environment. In general, the associated security capabilities are still somewhat basic. For example, in its capacity as a DMZ-based front end to the View Connection Server, the View Security Server from VMware merely offloads SSL processing. It doesn't even handle user authentication. And although this approach is somewhat decoupled from the application/server infrastructure, support is still limited to the applications hosted with the given VDI product.

IPSec VPNs—This approach also entails a standalone gateway and, as such, conveys benefits in terms of having decoupled infrastructure and easier configuration. The primary security features it provides, once again, are user authentication and encryption. Depending on the selected product, it might also support host integrity checking, network-layer firewalling, and some measure of network intrusion prevention. Another significant advantage is that like a private WAN connection, IPSec VPN enables access to virtually any electronic resource. In other words, it supports secure remote access for any and all types of VDI technologies that an organization might be running, in addition to all other services and applications that a user might need. That said, there are definitely some disadvantages to IPSec VPNs as well. First, they require special client software. This can be a major headache to deploy, only works for a subset of devices and platforms, and is impractical for non-employees and unmanaged devices. The second issue is that IPSec VPNs work by enabling a full network-layer connection. Therefore, additional containment infrastructure needs to be deployed to ensure that users—or worse, infected machines—do not overstep their intended access privileges.

Although they are achievable and perhaps even a good fit in limited situations, all of these options have one or more significant drawbacks. Fortunately, one approach still remains to be explored—a solution that exhibits all of the positive aspects of the other options and none of the negative ones.

The Strengths of SSL VPN Technology

SSL VPN technology is particularly well suited as a secure remote access solution for VDI based on the breadth and depth of security functionality it delivers, the ability to support multiple VDI methods and technologies at once, and the ability to address all of an organization's other remote access needs as well.

Robust security—In addition to flexible, multi-factor user authentication and encryption for all sessions, SSL VPN solutions typically support a wealth of advanced security capabilities, including host integrity checking; granular definition and enforcement of access policies; control over specific end user functions such as copy, print, and save; and extremely detailed logging/auditing of user activities.

In-depth support for VDI—Unlike some of the other alternatives, top-tier SSL VPNs are independent of the VDI technology/solution being used. This means there is no need to make any changes to an existing VDI implementation to get secure remote access to work. Yet, at the same time, there is no need to avoid changes, since the remote access infrastructure is capable of supporting multiple VDI solutions simultaneously. For example, an organization that starts out with a Microsoft-based VDI implementation does not have to worry about later adding Citrix XenDesktop and/or VMware View to its environment—at least not in terms of the impact this has on its secure remote access solution, because there isn't any. Furthermore, a decent SSL VPN solution also provides a range of value-added capabilities, such as single sign-on (SSO), smooth roaming (in the event of intermittent connectivity), and intelligent delivery of client software.

Extensive coverage for other needs—SSL VPN technology provides a secure remote access solution not just for VDI, but for all other types of resources and applications as well. This aligns favorably with the trend of widespread migration away from client/server and alternative architectures in favor of Web technologies. Enabling a wide range of access modes also ensures the ability to accommodate a broad array of client platforms, which is a key capability in this age of mobility and with the increasing prevalence and variety of user-owned devices (e.g., iPhones, Windows Mobile Phones, PDAs, and laptops running various operating systems).

The net result is that a leading SSL VPN solution has numerous advantageous. Chief among these is that it keeps users happy and productive—by giving them a uniform way to access all of the resources they need to get their jobs done—at the same time that it reduces cost and complexity of the organization's computing infrastructure and its operation.

Selecting the Right SSL VPN Solution

But not all SSL VPN products are created equal. Those with functional limitations or incomplete feature sets are not able to fully deliver the advantages outlined in the previous section. To guard against making a choice that is less than ideal, organizations should evaluate candidate products against the following criteria.

Comprehensive Access—Ultimately, the goal is to be able to provide any user—operating in any location with practically any type of device—access to just about any centralized computing resource. From a practical perspective such access is not always allowed, but the point is to at least have the capability so that it can be utilized when the need arises. From a technical perspective, this entails supporting enough access modes to account for all types of services and applications, including multiple flavors of VDI, as well as the leading third-party connection brokers. Furthermore, it is important to understand the dependencies and limitations for each of the access modes. What client operating systems are supported? What browsers are supported? What, if any, client software is required, can it be dynamically downloaded, and what technology (e.g., ActiveX) and configuration dependencies (e.g., user must have administrative privileges) are applicable? An ideal solution is one that incurs the fewest dependencies while still supporting all of the organization's access needs.

Comprehensive Security—Not only must data be protected while it is in transit and for whatever time it resides on a client device, but it is also essential to protect the organization's overall computing environment from remote systems that have been compromised or otherwise infected. In other words, security capabilities must be thought of in terms of providing end-to-end protection, and should ideally include the following countermeasures:

- Strong encryption for all access and administrative sessions
- Multiple authentication mechanisms, both for flexibility as well as to account for varying degrees of trust and risk
- Granular authorization/access control that can be dynamically adjusted based on a wide variety of attributes (e.g., user role and location, strength of authentication, ownership and security posture of the client device)
- Client-oriented features such as the ability to check the security posture of the remote device, the ability to clear the browser cache at the completion of an access session, and the ability to keep any downloaded data in an encrypted workspace, or else delete it once the session is terminated
- Gateway-oriented features such as a hardened OS, embedded firewalling, and mechanisms to thwart denial-of-service (DoS) attacks
- Detailed activity logging for both user and administrator sessions to facilitate troubleshooting and help demonstrate compliance with applicable regulatory requirements

Another security capability to look for is SSO. Ideally the implementation should be comprehensive in terms of addressing applications with a wide range of native authentication mechanisms (e.g., forms/header/cookie-based, Basic Auth, NTLM). Support for Security Assurance Markup Language (SAML), which can enable both intra- and inter-organization SSO, is also an increasingly important feature.

Transparency and Compatibility—On one hand this involves minimizing the effort and investment required by the users who need access. There should be no need to acquire, operate, and maintain any specific software or hardware at the remote end of the session. In addition, any dynamically downloaded software—such as agents or plug-ins used to support certain access modes or security features—should not disrupt or otherwise change the operation of any programs or the client system itself.

On the other hand, the same conditions should also apply to the party providing the access. The SSL VPN gateway should just “fit in.” Little, if any, network re-configuration should be required. Furthermore, it should be able to operate completely independently or, optionally, it should be able to take advantage of any existing credential and attribute stores (e.g., LDAP directories), access management software, and portal software that the organization is already using. Most importantly, it should not require applications and other resources to be modified in any manner in order to be remotely accessible.

Ease of Use and Administration—This category of criteria is somewhat similar to the previous one. However, in this case it is more about the day-to-day experience of the users, as well as the folks in IT/security operations. For the users, the key to success is ease of use. The interface should be intuitive, if not familiar, and very easy to navigate. Users should not have to sign on more than once in a given session. Nor should they have to make any decisions (e.g., in terms of the access mode to use), other than to select the resources they want to access. In the event that one or more groups of users have access to multiple resources, then a customizable, portal-style look-and-feel is appropriate.

For the administrators, it comes down to management functionality. A centralized management capability is essential, but it should also be possible to delegate policy creation to local administrators who might be more familiar with a specific group of users and the resources they are accessing. When it comes to the policy model there should be flexible grouping of related items, as well as reuse and modularity of object definitions and policy fragments. Overall, there should be an ability to implement virtually any access rule an organization can articulate. In addition, real-time session monitoring is helpful for troubleshooting purposes, while extensive logging capabilities are needed to support capacity planning and compliance reporting activities.

Performance—This category of criteria is intended to cover more than just system capacity, or throughput. Given today’s highly collaborative applications, latency requirements should also be considered when evaluating performance-related features—such as the count and type of processors being used, expandable memory, and enhanced techniques for handling and inspecting packets/sessions. The ability to ensure adequate capacity/performance for specific sessions—for example, by employing internal QoS or reservation techniques—would also be useful, particularly given the importance to any VDI initiative of being able to guarantee a positive user experience.

Scalability is another important factor, particularly when it comes to cost-effectiveness. This is determined in large part by a product’s management capabilities, but can also be affected by support for advanced features, such as clustering and virtual systems. The latter enables a single physical system to be used to provide access to multiple constituencies, but in a manner that keeps their policies, session processing, and activity logs separate from each other.

Finally, there is reliability, which continues to gain importance as providing secure remote access to computing resources is increasingly elevated to the status of “business-critical service.” In this case the primary feature to look for is support for multiple high availability configurations and mechanisms (e.g., active/passive, active/active, stateful failover, session persistence). Secondary to this is the inclusion of redundant components, such as fans, disks, and power supplies.

Summary

Virtual desktop infrastructure is rapidly gaining traction within modern IT organizations, primarily because of the plethora of technical, operational, and business-oriented benefits it provides. Representative solutions—such as those from Microsoft, Citrix, and VMware—enable delivery of desktops as a centrally managed service, driving down desktop TCO, bolstering data security, and enhancing the ability to respond to changing business conditions. Given the prevailing set of trends driving the simultaneous dispersion of users and centralization of corporate information resources, however, simple desktop delivery is no longer sufficient.

Going forward, achieving the full potential of VDI requires that IT organizations also establish a means to provide secure remote access to their centrally hosted, virtualized resources. In this regard, SSL VPN technology should be considered an ideal solution. By selecting a leading product, as defined by the criteria covered herein, organizations can efficiently provide secure access not just to their virtualized desktop environment(s), but also to all of the other applications and services that users need to get their jobs done.

About the Author

Mark Bouchard, CISSP, is the founder of AimPoint Group, an IT research and analysis firm specializing in information security, compliance management, application delivery, and infrastructure optimization strategies. A former META Group analyst, Mark has assessed and projected the business and technology trends pertaining to a wide range of information security and networking topics for more than 13 years. During this time, he has assisted hundreds of organizations worldwide with strategic and tactical initiatives alike, from the development of multi-year strategies and high-level architectures to the justification, selection, and deployment of their security and networking solutions. A veteran of the U.S. Navy, Mark is passionate about helping enterprises address their IT challenges.