SECURE ACCESS TO THE VIRTUAL DATA CENTER

Ensure that Remote Users Can Securely Access the Virtual Data Center's Virtual Desktops and Other Resources

Challenge

VDI is driving a unique need to extend ubiquitous access for company employees and enable a "local compute" feel while users are remote. Organizations need a unified system that can effectively manage and control access to their heterogeneous environment.

Solution

Juniper Networks MAG Series Junos Pulse Gateways or SA Series SSL VPN Appliances provide comprehensive secure access to virtual environments, including virtual desktops and servers, as well as access to Web applications, client/server applications, terminal services, and access from various mobile devices over a single platform.

Benefits

- Saves remote users time and improves their experience accessing virtual desktops
- Enables secure user access to various applications in addition to virtual-based ones
- Supports a variety of devices and operating systems
- Protects the network from users or devices that don't meet proper security credentials

Virtualization is one of the more common technology shifts in the data center space. One of the more interesting technologies being implemented in today's data centers is Virtual Desktop Infrastructure (VDI). VDI enables users to run personal computer instances (including applications, file access, and data) on a remote central server instead of on the hard drives of local PCs. Many companies are beginning to consider VDI because it will help them lower their administrative, support, and hardware costs associated with individual PCs. Additionally, virtual server farms, which are powering VDI and the overall data center compute environment, are increasing their footprint in today's data center networks. As companies begin to significantly deploy virtualization technologies in the data center, they will need an access solution that allows remote users to access virtual desktops and manage virtual servers securely and easily. In addition, companies will need a single remote access platform that can also handle users' access to Web applications, terminal services, client/server applications, and access from various mobile devices. This protects a company's investment over the long haul.

The Challenge

Companies are seeing the value of VDI and will begin to extensively deploy it over the next few years.

Currently, the two leading vendors in the virtual desktop infrastructure space are VMware (View Manager solution) and Citrix (XenDesktop solution). However, as virtualization begins to grow as predicted above, there will be more vendors offering VDI solutions in this market.

In order to meet this growth in virtualization, organizations will need a solid, secure, remote access solution that will allow seamless access for remote users to their virtual desktops, regardless of the vendor that they choose. However, it's not just remote user access to virtual desktops that organizations need to address. A company's remote access needs can evolve over time as applications that can be accessed are changed and/or users' remote needs change.

For example, this year a company's users may access the applications below in this allocation.

- 40% client/server applications
- 25% Web applications
- 20% terminal services applications
- 15% virtual desktops

However, next year the company's users may access applications in this new allocation:

- 30% client/server applications
- 35% Web applications
- 10% terminal services applications
- 25% virtual desktops

Bearing in mind changing remote access requirements, organizations must have a flexible and secure remote access solution in place to handle these evolving needs, while at the same time ensuring a consistent, simplified experience for remote users. During this rough economic period, organizations cannot afford to invest in multiple solutions as their remote access mix changes. They need a single remote access solution that is ready from day one to quickly address their remote access changes, is ready to support multiple vendors such as VMware View Manager or Citrix XenDesktop, and is ready to enforce comprehensive security checks on users and devices before granting access to corporate resources.

The Juniper Networks VDI Solution

Juniper Networks VDI Support with SSL VPN

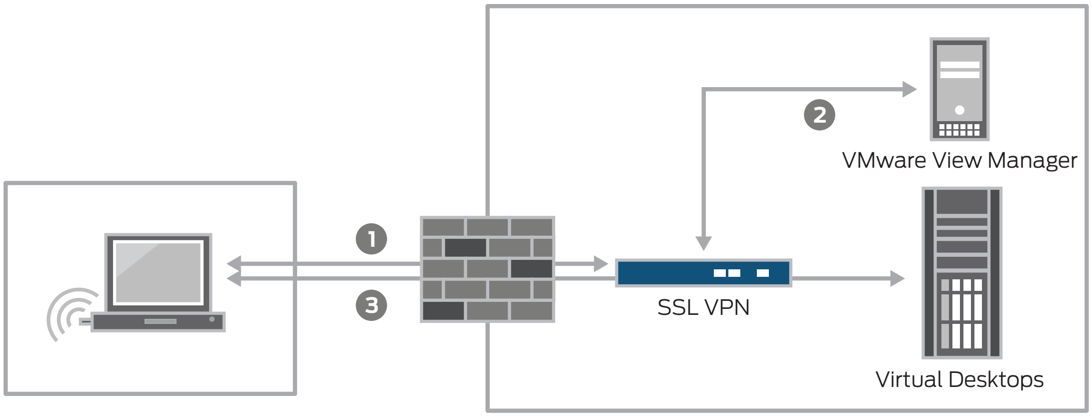
Juniper Networks® MAG Series Junos Pulse Gateways or SA Series SSL VPN Appliances interoperate with leading VDI products, including VMware's View Manager and Citrix's XenDesktop, to provide remote users with seamless, single sign-on (SSO) access to virtual desktops hosted on VMware or Citrix servers. This interoperability allows administrators to configure centralized remote access policies for users who access their virtual desktops. It also gives users a VDI client with which to access the virtual desktop, and it provides flexible client fallback options, simplifying deployment and management for administrators. This solution saves remote users time and improves their experience as they access their virtual desktops. Also, the MAG Series or SA Series offers this functionality to any and all internal VMware View deployments and other popular intranet applications—all from a single platform.

Figure 1 depicts how the Juniper's SSL VPN works seamlessly with VMware's solution to access virtual desktops.

Let's walk through Figure 1 in more detail. In the first step, the user (client) establishes an SSL VPN connection and the Junos Pulse session is launched automatically. The user is then signed into the network via single sign-on. Next the VMware View Manager provisions the virtual desktop from a preconfigured pool of virtual desktops. The user selects the assigned virtual desktop and this connection is brokered by the SSL VPN appliance. It's as simple as that to quickly gain access to virtual desktops. For users, this is a seamless connection to not only their assigned virtual desktop, but also to any other application or resource needed from the corporate network. And as companies' remote access needs change over time, the SSL VPN appliance is equipped to converge virtual desktop access, Web applications access, client/server applications access, terminal services access, and access from a myriad of mobile devices. All of these access needs can be handled on a single platform without any major forklift changes or any changes needed by the remote user.

Juniper Networks Virtual Server Administration Access with SSL VPN

MAG Series Junos Pulse Gateways or SA Series SSL VPN Appliances interoperate with leading virtual server products, including VMware vSphere, Microsoft Hyper-V, Citrix Xen, and IBM PowerVM. One of the new challenges with virtual server environments is securing administrative access into the virtual server farm. While virtual server environments provide enhanced administrative access methods, like the hypervisor layer controlling all VMs on a physical server that can be managed over a TCP connection, securing the management interfaces of this environment can be very challenging. Using SSL VPN,, organizations can strictly control which administrator groups can access what virtual server farm over which administrative interface, while providing a full audit trail log of the access privileges granted. Some of the access mechanisms offered by



1. Client establishes SSL VPN connection and MAG Series or auto-launched.
2. User is signed in using single sign-on. VMware View Manager provisions the virtual desktop from a preconfigured desktop pool.
3. User selects the assigned virtual desktop and the connection is brokered by the SSL VPN

Figure 1. SSL VPN in VMware View environment

SSL VPN connecting into the virtual server environment are the following:

1. Connect into Windows server VMs over a Remote Desktop Protocol (RDP) connection with RDP client applet provisioned by SSL VPN
2. Connect into Unix/Linux server VMs over SSH or Telnet SA provisioned client applet
3. Connect into Web administrative interfaces of servers through SSL VPN provisioned links menu
4. Connect into server environments using dedicated administration clients such as Windows Management Instrumentation (WMI)-based clients, VMware Virtual Center Client and the like, secured by Junos Pulse
5. Or natively allow super-admins network level access to the virtual server administration network over Junos Pulse, which allows for SNMP polling, and other direct access administrative tasks in the VM or even hypervisor environments

This set of capabilities forms a robust solution to provide controlled granular access into virtual server environments. This solution and set of capabilities can be used over the WAN for remote access, or over faster network connections to serve as the single portal for administrative access into the virtual server environment.

Figure 2 depicts how the SSL VPN works with virtual server environments.

Let's walk through Figure 2 in more detail. In the first step, the administrator establishes an SSL VPN connection and the start page containing all role-specific access provisions is presented. The user then chooses the virtual environment to be administered and launches the appropriate interface out of the following options:

1. User launches Junos Pulse client and launches the relevant administration tool (i.e., VMware Virtual Center Client). Every connection attempt by the administrator to the servers is logged.
2. User clicks on a link that leads to a web-based hypervisor administration interface. The IP addresses of the administrative Web interface does not have to be externally routable, as all links in the interface are rewritten and proxied by SSL VPN. Additionally, every action is logged to provide a full detailed audit trail record of administrative operations.
3. When the user clicks on an RDP or terminal applet link, a terminal or RDP applet is launched in a browser window and access to the management interface of the VM or virtual server is granted over the desired interface. Every connect and disconnect event is logged in detail.

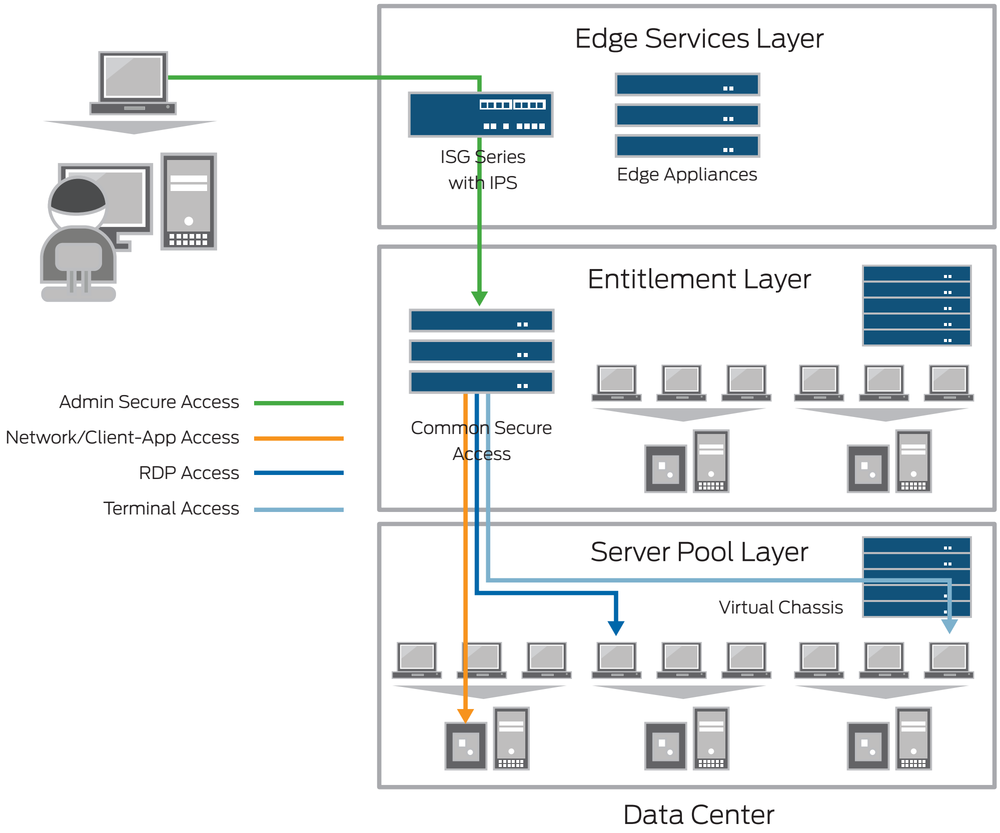


Figure 2. SSL VPN accessing the virtual data center

Features and Benefits

MAG Series or SA Series are the best way to secure and assure access to virtual data centers hosting virtual desktops and other applications, and they provide the following key benefits.

Long-Term Investment Protection

- Provide a single platform to access virtual desktops, Web applications, terminal services, client/server applications, and access from various mobile devices
- Enable companies to change their mix of remote access needs over time with a single solution
- Provide a consistent user experience regardless of how the remote access mix changes
- Result in lower costs vs. purchasing multiple remote access solutions to address different remote access needs

Improved Productivity and Ubiquitous Access to Virtual and Physical Environments

- Simplified access with single sign-on to virtual desktops to save users time
- Anytime, anywhere access using any Web-enabled device to keep users productive
- Broad cross-platform support including Windows, Mac, Linux, Symbian OS, iPhone, Windows Mobile, and others
- Access to diverse audiences (employee, contractor, partner) using a variety of devices (corporate laptop, home PC, smartphone, kiosk) from different locations (home, airport, hotel, office)

Easy to Deploy and Manage

- Plug-and-play connectivity; no software to deploy, install, configure, or maintain; no changes to existing servers; accessibility no matter what the platform
- Only a Web browser and Internet connection needed by user to simplify access experience
- Reduce ongoing support costs versus VPN (no desktop support calls)

Greater Security

- Provide robust endpoint security checks to ensure that only healthy devices are granted access to network resources
- Enable granular access control to users based on the user type, endpoint device, network connectivity location
- Assure a healthy device is logging onto the network by determining compliance before the user is allowed access
- Support endpoint health checking to significantly reduce the influx of machines infected with viruses, trojans, and bots—even from unmanaged devices like home and contractor PCs

Superior Reliability

- Proven solution deployed in tens of thousands of enterprises and service providers worldwide
- Market leader since SSL VPN category was created in 2002
- Recipient of numerous awards

Solution Components

The Juniper Networks SSL VPN solutions meet the needs of companies of all sizes. The solution uses SSL, the security protocol found in all standard Web browsers. The use of SSL eliminates the need for preinstalled client software, changes to internal servers, and costly ongoing maintenance and desktop support. The MAG Series or SA Series also offers sophisticated partner/customer extranet features that enable controlled access to differentiated users and groups without any infrastructure changes, DMZ deployments, or software agents.

Summary – The Most Comprehensive Secure Remote Access Solution for Virtual Desktops and all Remote Access Needs on a Single Platform

With Juniper Networks market-leading SSL VPN appliances, companies receive a long-term solution that will support VDI from multiple vendors, and they get the richest functionality for providing secure remote access for all of their users, regardless of location or endpoint device. In summary, Juniper Networks SSL VPN Appliances provide the following for virtual environments:

- A hardened security appliance, including Federal Information Processing Standards (FIPS) and Common Criteria solutions
- A single platform for all access methods
- A complete range of authentication methods: tokens, certificates, Lightweight Directory Access Protocol (LDAP), etc.
- SSO capability
- Documented performance and scalability
- Wide range of supported platforms
- Endpoint security scanning and validation
- Proven leadership in all verticals
- Detailed administrative and user logging   Integrated high availability
- Award winning platform

Next Steps

Please contact a Juniper Networks representative or Juniper's global network of channel partners for any questions about Juniper Networks MAG Series Junos Pulse Gateways or SA Series SSL VPN Appliances.

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at **www.juniper.net**.

Corporate and Sales Headquarters
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

APAC Headquarters
Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters
Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

3510352-002-EN July 2011

♻ Printed on recycled paper