

Force 3 VDI Teleworker Solution

The Telework Act of 2010 mandates that the head of each Federal agency develops telework policies that “ensure that telework does not diminish employee performance or agency operations.” This vague language has federal IT leaders scrambling to meet new requirements under some aggressive deadlines. The legislative deadlines, benefit/cost analysis and general management of a teleworking environment is one thing, but the demand to meet operational management and end-user expectations regarding ease of use, manageability and security is an entirely different task.

Teleworking provides a multitude of tangible benefits including higher employee morale, improved employee recruitment and retention, and increased productivity. Additionally, teleworking is an important component of continuity of operations (COOP) plans and an answer to the government’s initiative to make today’s data centers “green.” Difficulties in managing remote workstations, increased security risks with laptops, and IT funding for implementation have proven to be major barriers for government participation in teleworking. Virtual Desktop Infrastructure (VDI) is the key technology platform for breaking down those barriers by providing vital security components (the end device does not contain any user data), anytime anywhere access to the desktop via network or VPN and lower management, operational and support costs.

VDI centralizes physical desktops to virtualized farms in the data center that is then remotely accessed by end users through a host of devices, including zero clients (firmware based devices without any CPU, RAM or local storage), PCs, and tablets similar to the iPad. The resulting environment offers increased manageability, enhanced security, more robust data protection, and reduced support while at the same time providing anywhere, anytime access for teleworkers.

Force 3’s innovative approach to VDI combines the traditional benefits of VDI with proven enterprise remote access VPN technologies, resulting in a remote access architecture that enables reliable yet secure connectivity for VDI as well as, enabling secure connectivity for phones, tablets, or any device that a teleworker may be permitted to use to improve their productivity.

Force 3 Telework Architecture with VMware View

The Force 3 teleworker architecture for remote user support is based upon the Force 3 VDI reference architecture. This teleworking architecture simplifies end-user support and management by utilizing zero-client hardware and a pre-configured VPN router.

Key highlights of the Force 3 telework architecture includes:

- **Security** – The use of zero client hardware means that valuable data never leaves the data center. The PCoIP zero client does not store any data locally and is used solely as a graphical interface. With View 4.6, PCoIP protocol also supports SmartCard redirection, which is of importance for most of Federal agencies with increasing adaption of the HSPD12 directive mandating smart card login. Multi-layer security mechanisms will provide additional protection by limiting which devices can connect to the VPN router, and can allow only PCoIP

protocols to travel over the VPN tunnel. In all, zero clients and the Cisco ISE security management architecture provide best-in-class security for remote access solutions.

- **Ease of management and reduced support** – Components can be managed via a web-based console for simplified central management of thousands of teleworkers. The proposed solution allows zero touch provisioning. The VPN routers can be configured from a central configuration server minimizing manual intervention and reducing deployment costs. Using both the VPN router and zero-client hardware agencies can dramatically reduce support requirements.
- **Ease of Use by End-Users** – The use of zero clients with a centrally managed VPN router allows for simple “plug and play” technology for end-users to setup the telework environment remotely. A one-step plug in of the WAN port to the router and the end-user gains immediate access and use of the device. The telework environment is “instant on”, where a user does not have to wait for their PC to boot up.

Key components of the Force 3 teleworker architecture include:

- [VMware View environment based on Force 3 reference architecture for Federal Desktops](#)
- Cisco 881(W) Wireless VPN router for the teleworker’s home
- PCoIP Zero clients for telework’s home
- Cisco 3945 Series Router
- Cisco Identity Services Engine
- Cisco Configuration Engine

Enhanced security with PCoIP Zero Clients and multi-layer network security

Coupled with PCoIP zero clients, VMware View provides the ultimate security in the teleworking environment by completely removing access to the data from end-user devices, ultimately providing far greater security than laptops in a teleworking situation.

The Force 3 teleworking solution provides the following security benefits:

- The PCoIP zero clients are firmware based display devices that do not process or store data locally. End-users are accessing only the graphical display of the virtual desktop; no data is stored on the end-user’s hard drive. This prevents any data loss or introduction of malware into the corporate network.
- Desktop VMs hosted in the data center are maintained with current patches and are not dependent on end-users’ active involvement for downloads or updates.
- The Force 3 teleworking architecture provides multiple layers of security overarching the inherent security benefit of VDI. The Force 3 solution utilizes X.509 PKI certificates on the VPN routers to authenticate the IPsec tunnel, and 802.1X (a widely adopted IEEE industry standard) providing port-based access control for any endpoints connecting to the router including VDI clients, IP Phones, and Mobile devices. 802.1X is the [IEEE](#) standard for port-based network access control for enabling restricted use of IEEE 802 LAN service access points (ports) to secure communication between authenticated and authorized devices. The Force 3 solution centrally manages the list of authorized devices that can access the corporate network via 802.1X protocol or MAC Authentication Bypass (MAB). Firewall, IPS, and web content filtering are also integrated capabilities available on the 881W remote access VPN router.

Centralized management and reduced support cost

The key design point of the Force 3 teleworker architecture is ease of management and deployment. Both VMware View and the security management components provide a web-based console for centralized administration of all tasks. Deployment is eased by leveraging a dynamic VPN architecture that allows for a configuration template to be pre-loaded

before shipment of the router. Then upon receipt of the network equipment, zero-touch provisioning can be achieved, which minimizes the burden on the end-user during installation.

- The zero touch provisioning mechanism also greatly reduces the deployment burden of the IT staff. The plug and play technology results in end-users only performing one step to connect the router to the home network for an “instant-on” connectivity experience.
- PCoIP zero client reduces the support burden. Since the zero client is a display- only device, support is dedicated solely to hardware.
- The single pane-of-glass management console for VMWare View and security management solution will greatly increase administration efficiency.

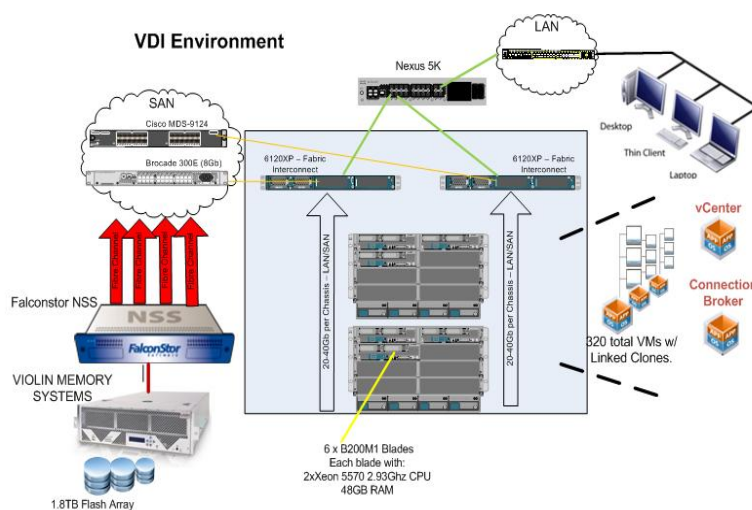
Ease of use

The foundation of the Force 3 remote access architecture is a remote-site presence of a Cisco 800 series router that provides network connectivity for VDI, voice, video and wireless back to the enterprise, enabling a true office-like experience for the teleworker. The teleworker would not need to perform any technical configuration or troubleshooting of the VPN device. Once the Cisco 881W router is connected to the teleworker’s home network, the PCoIP zero client and any other network devices such as an IP telephone can be connected to the 881W router via a hard Ethernet cable or a wireless network. This architecture provides a secure yet easy-to-support teleworker environment

Force 3 VDI Reference Architecture

The Force 3 VDI reference architecture with VMware View provides high end-user desktop performance by using Solid State Flash array as the storage for desktop VM Operating System images, specifically VMware View linked clones and replicas. Flash arrays will offer high Input/Output Operations Per Second (IOPS) at low latency. Even under heavy loads, flash arrays provide consistent performance characteristics rather than the exponential performance degradation experienced by spinning disks. The Violin Flash Array used in Force 3’s architecture will provide up to 200,000 IOPS and 20TB of SLC NAND storage in a 3U unit.

Remote display protocol that provides quality graphics and a multi-media experience is the key to end-user acceptance of the VDI solution. VMware View PCoIP (PC over IP) delivers a rich user experience over the IP network with progressive build, bi-directional audio and USB redirection in a completely new protocol. Internal Force3 testing indicates that PCoIP can provide 10x frame rate performance improvement compared to RDP protocol, thereby providing a greater end-user experience.



Conclusion:

The Force 3 telework architecture aims to provide end-users with an experience similar to that of a desktop and at the same time, provide a secure and easy-to-manage infrastructure. As the government IT landscape adapts to the changing needs of the federal worker, a VDI environment offers increased manageability, enhanced security and data protection, and new capabilities such as anywhere, anytime access for teleworkers.

Force 3's telework architecture will be provided as a bundled solution from Force 3 on the NASA SEWP IV contract as a single line item purchase that includes product, services and training. The bundled approach reduces risk, time to benefit, and cost for Federal agencies looking for teleworking solutions. For customers with existing infrastructures, customized product/service offerings are available to reduce the implementation cost.

About Force 3:

Headquartered in the Washington, D.C. area, Force 3, a VMware Premier Partner, has been inspiring customer success for 20 years. We have nearly 300 employees across the country who are driven by innovation and creativity, working everyday to ensure that our customers achieve their mission requirements.

What does this mean for our customers? Our engineers have the expertise to enable your solutions to work better together. From day one, our data center practice has been built around virtualization technologies, with our team of engineers working constantly to bring customers the latest technological advances and success. For more information, please contact Sudhir Verma, Senior Director of Consulting Services, at sverma@force3.com.



LEGAL DISCLAIMER

VMware, VMware View and VMware vSphere are registered trademarks and/or trademarks of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. VMware warrants only VMware products and services to the extent set forth in the express warranty statements accompanying such products and services. The use of the word "partner" or "partnership" does not imply a legal partnership relationship between VMware and any other company.