

FREQUENTLY ASKED QUESTIONS – SECURING AND MANAGING THE MOBILE WORKFORCE, INCLUDING EMPLOYEE-OWNED DEVICES

Companies globalizing their businesses or supporting a highly mobile workforce face the challenge of making these mobile users just as secure and productive as those employees at the main offices. Furthermore, with the rampant adoption of smartphones and iPads, including those owned by the employees, and more users using them for business purposes, IT managers wonder how they can secure and manage these devices just as they do corporate laptops and desktops.

How do you ensure remote end-user satisfaction with the remote access performance and availability worldwide?

Providing consistent and high quality remote access connections anywhere in the world that are available at all times is a non-trivial task for most IT managers. In many situations, the easiest, quickest and most cost-effective option is to consider a managed SSL VPN service that has the following capabilities:

- **Global Redirect.** Consider MSPs that have data centers in various regions of the world with the ability to route your traffic to the closest data center to take advantage of the performance of its private backbone network. In this way, the end user's exposure to the public Internet is minimized, and the result is a better overall experience.
- **Global Load Balancing.** If guaranteed high uptime is important to your business, evaluate an MSP's ability to load balance between diverse data centers in a region as well as between geographic regions. Data center diversity coupled with load balancing can significantly increase uptime. And don't hesitate to ask for SLAs, even 100 percent uptime SLAs.
- **On-demand Capacity.** To address business continuity needs, look for on-demand capacity via a capacity reservation feature, providing the ability to immediately increase the number of end user seats needed to keep up with a spike in demand during a business continuity event such as a snow day, hurricane, flood, pandemic, or man-made disaster. This eliminates expensive capacity overbuilds while maintaining end user productivity.

Download an executive brief on [How to Improve Remote User Satisfaction and Maximize ROI by Using SSL VPNs for Mobile Access, Telecommuting, and Partner Extranets](http://www.virtela.net/resource-center/whitepapers/more-whitepapers/improve-roi-with-ssl-vpn) at www.virtela.net/resource-center/whitepapers/more-whitepapers/improve-roi-with-ssl-vpn.

How do you provide immediate scalability for remote users in case of a business continuity event?

Look for solutions that have the ability to reserve capacity in order to scale quickly to support additional users. One can purchase dedicated SSL VPN gateways and emergency licenses from SSL equipment vendors, however, these licenses typically are expensive and have time limit on how long they can be used (e.g., two months) before you need to purchase a new license.

Consider a managed service, hence eliminating upfront capital expenses and opex to manage the solution. Additional capacity can be reserved when unexpected spikes in traffic happen due for example, in the event of a natural disaster, when many users may need to work remotely. The on-demand capacity feature ensures that remote users can connect and remain productive without having to over-engineer the network to support the temporary increase in traffic.

Learn more about [Virtela's Managed Cloud-based SSL VPN service](http://www.virtela.net/services/remote-access-services/ssl-vpn) at www.virtela.net/services/remote-access-services/ssl-vpn.

Can you prevent infected remote end users from spreading viruses and worms to the rest of the corporate network?

Choose a remote access service that provides a layered security approach, with SSL VPNs as a method of securing access, and firewall and Intrusion Prevention System (IPS) services providing an additional layer of security. The SSL VPN acts as an access control enforcement point, looking at the security posture of the device attempting to connect, block, or limit access if a security control is not in place such as the most up-to-date anti-virus enabled on the endpoint. Firewall and IPS services provide additional layers to prevent unauthorized access plus prevention against worms, viruses, Trojans, and other threats from entering the corporate LAN and infecting your network.

There are a number of point vendors available for SSL VPNs, firewalls, and IPSs with different feature sets, areas of strength, and price points. A Managed Service Provider (MSP) option provides an alternative for companies that may have limited capital to buy,

or resources to integrate, manage, and maintain devices at the premises. Furthermore managed cloud-based versions of these services allow you to turn services on (and off) to secure new locations and/or enable more robust security, as you need them.

Download the CTS Corporation case study at www.virtela.net/pdf/CTS_CS.pdf. CTS designs, manufactures, and sells a broad line of electronic components and sensors, and a provider of electronics manufacturing solutions (EMS) globally.

Can you quickly produce meaningful log data in the event of a forensic activity?

It's not enough to just collect log data from security devices. The data needs to be correlated across the devices with alerts generated to signal a threat to the network and log storage is needed for a year or more depending on specific compliance activities. In the event of a security breach, you need quick access to log data to identify and mitigate the source and destination of the threat so that the threat can be blocked and potentially compromised resources can be identified. If you don't have a good log management system, identification of the logs can take a long time and there's no guarantee you will find what you need.

Consider managed SSL VPN and security services with integrated Security Information and Event Management (SIEM) capabilities. SIEM includes log retention and management, providing retrieval of log data, as needed, in order to facilitate compliance activities or in direct response to a forensic activity. This reduces the time required to sift through large amounts of data to try to get to meaningful information so that you can take appropriate action.

Learn more about Virtela's Managed Cloud-based SIEM service at www.virtela.net/services/security-services/siem.

Would you know if an employee installed a rogue app on their smartphone making them noncompliant with your acceptable use policy?

Choose a mobile device management (MDM) platform that allows you to specify the parameters and thresholds for your acceptable use policy such as which apps are allowed or are required on the device, and which apps are forbidden such as those known to host malware or interfere with productivity such as Angry Birds. The MDM platform must have the capability to detect applications that fall outside of your acceptable use policy, alerting IT managers who can then work with the end user to remediate.

There are number of MDM platforms in the market with a wide variety of features to evaluate. For companies that may not have the capital to buy as well as the resources to maintain and manage the platform, consider evaluating MDM services from Managed Service Providers (MSPs). Some MSPs offer managed cloud-based MDM services to solve upfront capital and resource constraint issues. Cloud-based MDM services can also be activated instantly and provide a range of service options from self-serve to full management of end user mobile devices.

Learn more about Virtela's Cloud-based Mobile Device Management service at <http://www.virtela.net/services/mobile-device-management/cloud-based-mdm>.

ABOUT VIRTELA

Virtela Technology Services Incorporated is the world's largest independent managed network, security and cloud services company. Virtela offers an award-winning suite of services – including managed networks, security, application acceleration and proactive infrastructure management – to mid-market and Fortune 500 customers around the world. Virtela offers unparalleled geographic reach to more than 190 countries through its partnerships with more than 500 carriers.

Virtela is headquartered in Denver, Colorado, with globally distributed Network Operations Centers in the U.S., India and the Philippines. For more information, please call +1 (720) 475-4000 or visit www.virtela.net.