

# National Webcast Initiative

## Wireless Security Wire-Free Does Not Always Mean Risk-Free! Wednesday, July 20, 2005

---

*These resources are provided because they have information that may be useful and are provided as a general reference only. We do not warrant the accuracy of any information contained in the resources.*

### Providing endpoint security for remote VPN users

**The dispersal of viruses, Trojan horses, worms, and other security threats over the public Internet has increased with alarming frequency. As remote user VPN deployments over public networks have become more widely deployed, the issue of endpoint security has moved to the front of every IT and network administrator's agenda.**

**Users should implement a PC Client capability that addresses this risk by enforcing endpoint security for remote VPN users.**

In today's world of widespread viruses and worms, even the most well-intentioned user can become a threat to network security. That's why enterprises need a "tunnel guard" facility to provide endpoint security for remote PCs within their virtual private networks (VPNs). This capability needs to provide a comprehensive security solution, capable of enforcing security best practices on both managed and unmanaged (IPsec and SSL VPN) endpoints. This technology should also enable the administrator to define endpoint security policy on the VPN gateway itself and ensure all users or devices connecting to the VPN gateway are inspected for compliance to the policy. Users can be denied access or have access restricted based on compliance status.

A capability such as this helps to prevent the end-user PC from becoming a vehicle for viruses or other unwanted intrusions into the secure enterprise network through the VPN tunnel.

Needed benefits:

- > Provide remote endpoint security for both SSL and IPsec end points
- > Validate the presence and status of any application or file type on the user's device
- > Initiate remediation and quarantine of users who don't adhere to security policy
- > Inter-work with 3<sup>rd</sup> party security vendors by offering an open API

The above set of VPN safeguards protects against malicious intent and user negligence. This is especially critical when providing SSL VPN access from devices that the enterprise doesn't own or control like public internet kiosks or home PCs. For example, administrators can create dynamic access policies that can be used to specify restricted levels of access or even deny access altogether based on user parameters such as type of device, user IP address, or type of authentication being used. Whenever a new SSL VPN session is established, a cache-wiper feature should be enabled within the browser to clear all cached content and browser history upon session termination. And to help prevent a scenario where a vacated kiosk holds an open session, any inactive SSL VPN connection should be terminated after a brief countdown warning. This feature reduces the chance that a subsequent kiosk user could get access to the previous user's confidential session.

This type of feature checks the security status of the endpoint, including the status of executables, files, registry values, versions, patches, and operating system configurations prior to granting an endpoint network access.

An implementation of such a capability would consist of two key components:

- A *software requirement set (SRS)* which is configured and most likely runs on the VPN Gateway/Router. The SRS specifies the software an end-user PC must be running as a prerequisite to admitting an end-user tunnel. The requirement set can include multiple programs and the ability to specify alternatives. The ability to specify version levels of the software and whether the software is actually running is also included.
- And the *agent* that runs on the user's device (either pre-installed or downloaded automatically from the VPN Gateway/Router). This agent monitors the PC's operating environment to detect whether particular software applications (e.g., personal firewall or virus checker) are installed and running. Not only are the programs verified, but the VPN Gateway also determines that they have not been compromised.

### **Don't take chances**

IT administrators can't always keep their remote users free of viruses, but they can keep them from infecting the network. By implementing the above suggestions, enterprises can reap the economic benefits of virtual private networking with much lower levels of security exposure.