Intel IT Center

DECEMBER 2013

Mobile Productivity: Solution Spotlight

Cisco AnyConnect* Delivers Stronger, Simpler VPN Security

Russell Rice, *Senior Director, Secure Access & Mobility Group, Cisco*

Russell Rice explains how Cisco AnyConnect* Secure Mobility Client–based solutions enhance the VPN experience.

Today, companies around the world are grappling with how to deal with the risk of workers using mobile devices, especially those that are personally owned. One of Cisco's goals is to provide IT with security controls that enable a seamless mobile experience.

An important element to protecting access is ensuring that an organization can securely identify both the user and the device, and do so without overburdening the user with constant requests to manually authenticate. That is where Cisco and Intel have teamed up to provide a great solution.

With AnyConnect* solutions running on Intel® architecture-based mobile devices, users have simpler access to the tools and information they need to stay productive.

A "No-Password" VPN Experience

Enhancements in the latest 4th generation Intel® Core™ vPro™ processor make the sign-in process even easier. When organizations are using Intel Identity Protection Technology[1] with Public Key Infrastructure (Intel IPT with PKI) and running Cisco AnyConnect Secure Mobility Client with Cisco* Adaptive Security Appliance (Cisco ASA), they can enable secure two-factor authentication without the need for additional VPN login credentials.

4th generation Intel Core vPro processors deliver a "no-password" VPN experience so that users can simply log into their device and connect to the VPN through their AnyConnect* client without having to enter another password. The Cisco ASA authenticates against the certificate and eliminates the need for a dedicated VPN login password.

Faster Two-Factor Authentication

At the heart of the no-password VPN experience is a two-factor authentication technology that does not compromise on security. Cisco AnyConnect Secure Mobility Client–based solutions work together with Intel IPT with PKI to deliver hardware-enhanced authentication security across the enterprise, helping to reduce costs and minimize risk. Intel IPT with PKI works on two levels:

- It prevents screen scraping with hardware-based protection that hides a user's keystrokes.
- It stops illegitimate users from logging in. It does this by generating a secure token for each user or device that validates that a trusted person (not malware) is logging in from a trusted device.

intel Look Inside.™

Cisco and Intel: Securing a Mobile Future

Cisco is committed to providing the tools to make sure that the right user, on the right device, is granted the right level of network access—from any location. And this is accomplished by providing organizations with the seamless connectivity, visibility, and control of all users and devices, at all times.

I'm pretty excited about what Cisco and Intel have been able to put together to create stronger mobile security. With AnyConnect solutions running on Intel architecture-based mobile devices, users have simpler access to the tools and information they need to stay productive, while IT gains the comprehensive, built-in security[2] that the business requires. The solution also helps keep operating costs down by reducing requests for IT support.

Moving forward, Intel and Cisco will continue to work together to make mobile security even better. This includes broadening the footprint of mobile devices and improving the experience for both virtual and application-centric technologies.

Additional Resources

To learn more about Cisco AnyConnect* Secure Mobility Client–based solutions, go to cisco.com.

To find out more about mobile devices based on Intel® architecture, visit intel.com/mobileproductivity.

Share with Colleagues

[1] No computer system can provide absolute security. Requires an Intel Identity Protection Technology–enabled system, including an enabled Intel processor, enabled chipset, firmware, software, and Intel integrated graphics (in some cases), as well as a participating web site/service. Intel assumes no liability for lost or stolen data and/or systems or any resulting damages. For more information, visit http://ipt.intel.com/. Consult your system manufacturer and/or software vendor for more information.

[2] No computer system can provide absolute security under all conditions. Built-in security features available on select Intel Core processors may require additional software, hardware, services, and/or an Internet connection. Results may vary depending upon configuration. Consult your system manufacturer for more details. For more information, visit intel.com/technology/security.

1213/CP/ME/PDF-USA 329917-001

intel Look Inside.™