From Remote Access to Secure Mobility: Enabling Next Generation Workforce Productivity

Why Mobility Matters

Technology has always ushered in new opportunities for productivity enhancement. Companies that can embrace and exploit technological innovation, particularly its disruptive aspects, typically win in the market or capture market share over those that cannot. Today, a new wave of technological disruption is upon us: the hyper-extension of corporate mobility—enable employees to work from anywhere at any time.

Corporate mobility is not new for enterprises. In fact, remote access and telecommuting solutions have existed for quite some time. But what is new is the astounding rate of change in corporate mobility platforms and the ability for the enterprise to support it, coupled with the fact that the change is being ushered in by employees, not the traditional IT group.

Corporations must embrace mobility to remain competitive and evolve to a new model of efficient workloads. In today's lean economic times, downsizing and global outsourcing are the norm; companies must do more with less. Embracing mobility is in the best interest of corporate organizations as it leads to even greater productivity than what we have achieved with the Internet.

Not only is it imperative from a competitive standpoint, but the shifting demographics of today's workforces also demand it. As baby boomers retire and become a smaller part of the working population over the next 20 years, the gen Y and millennial generations will rapidly grow to equal and surpass the generation X subset of workers in our global society. These generations believe in the social web, Internet communities, constant communication, and information exchange. Many of today's younger workers have been brought up with such a pervasive Internet connection that making use of their ability to be "always on" for corporate purposes has the potential to create a huge boon in productivity.

Challenges of Embracing Mobility

Enterprises have spent millions of dollars enabling remote connectivity by creating network and security infrastructures, then poking deliberate holes through their borders. In fact, VPNs have played a major role in enabling laptops to become the mobility device of choice. However, this is rapidly changing. As smartphones and tablets surpass the compute power of the traditional PC-based devices from only a few years ago, their richer, better-designed user interfaces, their place as the voice communication device in the case of smartphones, and their built-in support for pervasive wireless connectivity are quickly making them the employees' devices of choice.

Perhaps the biggest challenge enterprises face is the loss of control. In this new world, consumers, who are also corporate employees, are pushing the agenda. They are voting with their dollars for devices with slicker interfaces, a better user experience, and more convenience. Employees are finding ways of enabling these devices—sanctioned or unsanctioned—on their corporate networks, and corporate standards that encumber this are quickly sidestepped.

The speed with which change is happening is also challenging for the enterprise. Corporate IT groups must adapt quickly to a proliferating set of new mobile platforms; they must reassess their security posture and framework in relation to new devices. Consumers are adopting new technology faster than standards are being developed, and the tools designed to help manage the onslaught of requests for support of these new mobile form factors are behind in keeping up.

Perhaps the most basic challenge is in securing the new modes of access. Fundamentally, the old security paradigm—“crunchy on the outside, mushy on the inside”—is no longer valid in today’s mobility environment. The perimeter boundary is truly gone and the network edge is everywhere, even in the palms of mobile employees’ hands. What are the corporate liabilities of losing these mobile devices? What role do they play in introducing traditional security threats into the network? Corporations likely have the infrastructure to deal with these issues for some form factors, like PCs, but for newer form factors, corporations lack the capabilities to protect corporate data, secure their networks, and provide adequate service levels for application access.

The Answer: Secure Mobility

Enterprises and their IT groups need a framework and solutions to securely enable mobility. At Cisco, we believe the answer is secure mobility—providing access, security, and choice:

- Easy **access** to applications and information that users need to do their jobs
- Accurate **security** to protect endpoints from threats and to enforce corporate policy on devices
- The ability to support a wide variety of devices in order to provide users with a **choice** of which tools to use

These fundamental characteristics establish the foundation that enterprises need to embrace mobility.

Cisco’s Value Proposition

Cisco is ushering in secure mobility, delivering a network posture that enables “anywhere, anytime” optimized connectivity for anyone related to a company’s activities. Cisco® AnyConnect Secure Mobility solution sits within this framework as a set of solutions designed to seamlessly and securely enable the mobile workforce. The AnyConnect solution consists of a Cisco ASA series appliance, Cisco AnyConnect Secure Mobility client and web security enforcement with either Cisco IronPort Web Security Appliance or Cisco ScanSafe.

AnyConnect Secure Mobility Solution

Cisco AnyConnect client is a unified endpoint software client that is compatible with all of today’s major enterprise mobility platforms (PCs and smaller form factors). Built on foundational VPN technology, AnyConnect Secure Mobility solution extends its value proposition beyond remote access to leading-edge user friendliness and state-of-the-art network-based security. Sitting on endpoint computer devices, AnyConnect Secure Mobility enables security in the network fabric behind the firewall and provides unprecedented security and corporate policy enablement when users are mobile, outside of the corporate firewall.

The next section takes a closer look at the security challenges enterprises are facing in enabling mobility and the opportunity for AnyConnect Secure Mobility solution to help bridge the gap between today’s reality and the promise of secure mobility.

Pitfalls of Enterprise Mobility Enablement

The VPN Opening—While providing flexibility for mobile workers, the VPN is perceived as one of the biggest security holes in enterprises today. After companies spend countless sums on fortifying their Internet edge perimeters, they fail to realize that laptops now form part of that edge. When Internet activity is channeled through the corporate network, additional web proxy technology can block out harmful sites. Most VPN clients on the market today can be cumbersome for end users, often requiring repetitive tasks for initiating sessions. This fact, as well as bandwidth considerations, causes end users to roam freely on the Internet without the VPN initiated. The effective split tunnel caused by non-protected Internet surfing introduces the opportunity for malware to infect an endpoint and later propagate itself on the corporate network once that device is allowed back on.

The Cisco AnyConnect Secure Mobility Solution helps plug legacy VPN openings. In 2010, Cisco became the first vendor to introduce a cross-platform solution for PCs (Windows, Mac, and Linux) that included a configurable, persistent VPN plus integrated web security. When running in “always on” mode, the AnyConnect solution facilitates consistent usage and a security policy enforced through the Cisco IronPort® Web Security Appliance. Cisco AnyConnect client authentication credentials apply specific web usage policies and security that can vary based on the location the user is connecting from (inside or outside the physical corporate perimeter).

The “Dark Web”—Given the explosive growth of web domains, most of the Internet remains unclassified. And most PC endpoint infection today is propagated through malicious websites. Correlation or active scanning are vehicles for more accurate classification of IP addresses that are part of the Dark Web. Cisco uses its industry-leading web reputation filtering and dynamic on-the-fly classification technology to make sense of these websites. Over time, Cisco’s Security Intelligence Operations (SIO) center enacts global correlation of the IP information gained from most of Cisco’s security appliances and products.

The Port 80 Portal—Despite years of acknowledging TCP-based applications such as instant messaging as ripe grounds for endpoint security infection, the problem has only gotten worse. With today’s Web 2.0 applications fostering new levels of fast communication and social interaction, the potential for malicious links and security threats has never been greater.

AnyConnect Secure Mobility solution ensures that all endpoint traffic traversing port 80 is deeply inspected for malicious content. In addition, a consistent security policy based on user or group identity can be applied, which allows or denies access to specific web applications.

The SaaS Leak—An adjunct trend that has helped accelerate mobility has been the movement of corporate applications outside of the internal data center. Applications that live on the web can be accessed from any device that supports an Internet connection and provides access to a browser. Due to this trend, corporate data is increasingly sitting behind public Internet sites that host software-as-a-service (SaaS) business applications. IT groups may even be unaware of the full extent of use of SaaS applications within their corporate installed base. Even for sanctioned and supported SaaS applications, the ability to monitor and manage access to these distributed applications can be daunting. AnyConnect Secure Mobility solution uses Security Assertion Markup Language (SAML) to create a single point of authentication revocation and management for SaaS applications. For supported applications, end users benefit from not needing to remember yet another password and seamlessly entering key SaaS applications if their IT group has not disabled their access.

Device Loss—A lost or stolen smartphone or tablet can be devastating to its owner, causing loss of money, loss of personal and corporate information, and loss of productivity. However, the operational challenges and potential legal ramifications for the business are much worse. The loss and potential misuse of sensitive information stored on the device and the potential for the device to be used to gain access to critical business systems can force a company to spend thousands, if not millions, in incident response, information and system recovery, and responsible disclosure costs.

To provide a first level of protection if a mobile device is lost, comprehensive device security should be enforced for all mobile users who access corporate information. Cisco AnyConnect Secure Mobility solution supports the use of digital certificates, which can be revoked immediately when devices are lost, denying access to the network. Policies like PIN lock, device encryption, and not “jailbreaking” phones will help secure a device even if it is lost and will reduce the threats that can be introduced as mobile OS platforms are opened up. Every organization must determine which smartphone and tablet policies they require, and must work with each platform’s capabilities to enforce that level of security. Many companies will find Exchange ActiveSync sufficient; others will need the advanced features of a mobile device management solution to complement and enhance AnyConnect’s built-in device security features.

Consumerization of IT—Companies used to dictate the type of IT equipment an employee would use. By doing so, IT could maintain control over the device and the endpoint, thus ensuring that a consistent security was enforced. IT is now moving toward a model where the employee either purchases their own mobile device or IT reimburses the purchase of a device. Either way, the employee chooses the device that they would like to use on the corporate network. The cost of this flexibility and choice for the employee is that IT can no longer dictate what image will be on each device, because each device is individually owned.

AnyConnect Secure Mobility solves this problem by making the AnyConnect client available on each endpoint. Broad device support for laptops, smartphones, and tablets means that the basic secure connectivity can be easily enforced and always on. In addition, the underlying web security from the Cisco Web Security Appliance or ScanSafe ensures consistent policy enforcement, whether the user is accessing information in the office or remotely.

Conclusion

Instead of fighting IT consumerization and the associated flood of new mobile devices, connections, and applications, the enterprise must embrace the mobile environment as a model through which employee and partner productivity and creativity can flourish. Mobility is here to stay, and it is up to IT departments to find a way to consistently enforce security on those mobile devices.

With Cisco AnyConnect Secure Mobility, companies can embrace mobility and leverage their existing infrastructure and processes to provide secure access to anyone, anywhere, anytime, from any device.

To learn about Cisco AnyConnect Secure Mobility Client, please visit
http://www.cisco.com/en/US/netsol/ns1049/index.html

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C11-641140-01 04/11