celestix

WHITEPAPER

How to benefit from secure DirectAccess connections

Published July 2011

Contents

Introduction

Background structure of DirectAcess

The user, IT, and security with DirectAccess and HOTPin

The user
IT administration
Security for IT and users

Contact information

Introduction

On a busy summer day in Los Angeles, a traveling executive stops at a sidewalk café equipped with Wi-Fi so she can respond to some urgent emails before moving on to her next appointment. She orders a latte and a croissant and then powers up her laptop. After logging on to her system she is automatically prompted for a network login password. She reaches for her smartphone and uses HOTPin™ to generate a dynamic one-time password (OTP) which she enters with a PIN to access her company network. The interaction between user and system is simple and efficient.

What the user doesn't know is that both she and her machine have just authenticated via DirectAccess which is built on a foundation of proven standards such as Internet protocol version 6 (IPv6) and IPsec. She now has the full work capabilities as if she were in her office.

What the user does know is that she can securely sign off on the payment reports that require her approval while she enjoys her meal. With access to all of her authorized applications and files, she sits at the café sipping her latte and efficiently completes her work. She can travel and meet deadlines with ease.

She doesn't know that Microsoft's DirectAccess is the feature that provides the 'always on' user experience that enables remote users to access enterprise resources without the need for third-party client connectivity software.

She may not realize that HOTPin allows her to login more securely while she travels. Were it not for HOTPin, if someone stole her laptop and gained her static password, that person could access the company's network uncontested. HOTPin challenges every remote user to properly authenticate. She doesn't know how this is possible, just that she is far more productive when she can get her job done from wherever she needs to be.

For her IT counterpart back at the corporate offices, the 'always on' solution combines a trio of successful implementation factors: seamless user experience, ease of management, and strong security. Historically, one of these functions suffered at the hands of one or both of the others. How these three elements interact with each other defines a security solution's efficacy and success. To get a better idea of what this technology can do to secure network access, let's take a brief look at the structure of DirectAccess and HOTPin.

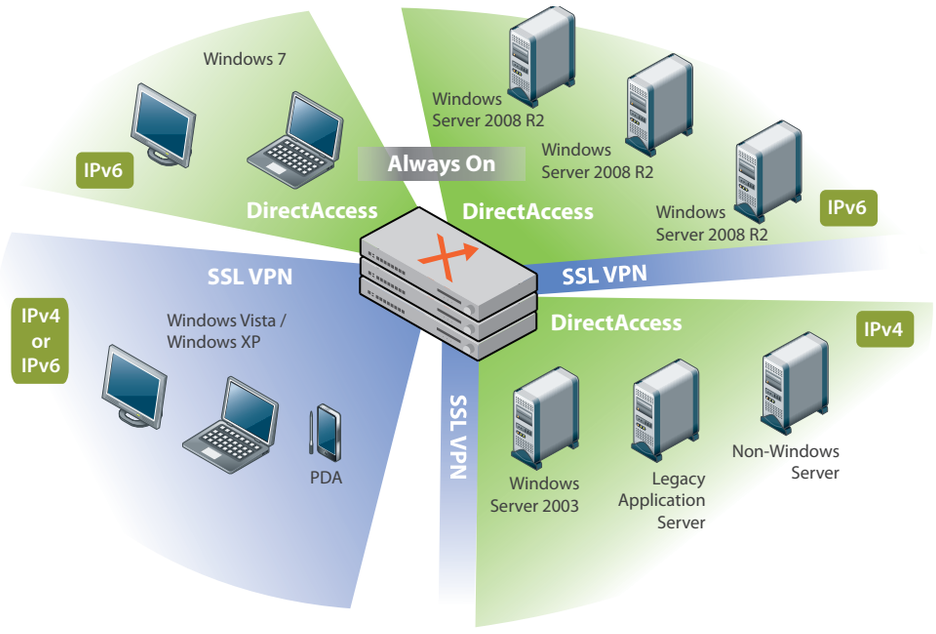
Background structure of DirectAccess

Any discussion about DirectAccess (DA) must focus on the connection, formally defined as *an always-on IPv6 IPSEC-style connection without the need for a VPN*. Introduced by Microsoft®, DirectAccess is a feature available in Windows® 7 and Windows Server® 2008 R2. The best implementation combines DirectAccess with Microsoft Unified Access Gateway 2010 (UAG) installed on a Celestix WSA Appliance. In operation, DirectAccess allows trusted remote workers to rapidly access the entire corporate environment regardless of location.

UAG is the obvious enabler for providing access control for both trusted devices using DirectAccess and untrusted devices that are not. UAG provides unparalleled network access options via SSTP, remote desktop gateway, Secure Socket Layer (SSL) VPN, and Network Connector. In addition, UAG can be integrated with

Network Access Protection to provide session-persistent endpoint compliance and protection. It also empowers IT to apply granular policies based on the trust level of the endpoint and type of application being accessed.

And UAG is more than just an access gateway, it can manipulate application data in real time. If a user logs in remotely from an untrusted device, UAG applies policies at the gateway that limit network access. UAG establishes a bi-directional connection with the user's enterprise network each time their DirectAccess-enabled portable computer connects to the Internet. The good news for IT teams: The DirectAccess solution scales to meet enterprise needs.



In the diagram above, the DirectAccess-enabled computer connects to the enterprise network as soon as it identifies an Internet connection. DirectAccess establishes two separate IPsec VPN-style tunnels (data pathways) between the enterprise network and the remote computer. The infrastructure tunnel (also called the 'machine tunnel') communicates with Active Directory ® (AD). The second tunnel (also called the 'user tunnel') enables user access to all enterprise resources. This construct leverages AD, Group Policy, and other applications. Neither tunnel requires VPN setup.

DirectAccess utilizes the IPv6 protocol, so companies looking to benefit from it must consider how they will manage traffic from remote user PCs to their IPv4-enabled network.

One option would be for the company to upgrade their infrastructure to operate with IPv6 addresses, but this is a complex, time consuming and costly approach. The simpler alternative is to leverage Windows Server 2008 R2, which resides on the Celestix WSA appliance and readily translates IPv6 protocol to IPv4. This allows companies to benefit from DirectAccess without having to upgrade their internal systems.

UAG thus provides IT teams the simplest, most cost-effective platform for realizing the benefits of enabling DirectAccess. The only other way to deploy DirectAccess (other than with UAG) is to upgrade all network devices to IPv6 addresses.

DirectAccess provides significant operational advantages to organizations with a remote workforce. However, some industry pundits have expressed security concerns about providing users with laptop devices that have an 'always on' connection to the network. Organizations that elect to leverage DirectAccess must give careful consideration to how they authenticate and control access from enabled devices.

The user, IT, and security with DirectAccess and HOTPin

The user

The DirectAccess user relates to IT almost transparently. Simply put, DirectAccess is always on, always accessible to a user registered in Active Directory who has Internet access. In one scenario that could compromise network security, a thief steals a DirectAccess enabled laptop, hits an internet access point and attempts to gain access to the network.

Administrators can mitigate this risk by configuring DirectAccess to prompt for user credentials before network access is granted. The HOTPin one-time password further enhances the security by providing strong two-factor authentication that integrates seamlessly with DirectAccess.

With HOTPin, a user obtains a one-time password through two main communication methods: a smart device client (for example Windows Phone 7, iPhone®, Blackberry®, Android™, iPad®, etc) or SMS (text message).

HOTPin replaces dedicated one-time tokens with a software token, referred to as a 'soft token.' HOTPin technology leverages the enterprise's investment in users' smart devices as a cost-effective solution.

Whenever any user accesses the network remotely over the internet, that user has the same experience and access as though sitting at her desk in the corporate office. Security operations including machine and user authentication are seamless and fast, making IT nearly invisible to the user.

IT administration

With UAG and DirectAccess, corporate IT can manage and authenticate all machines and remote users associated with the network. IT experiences happy users, which translates to sharply reduced help desk and support calls for login and network access issues. In addition, an administrator can use the 'manage out' feature of DirectAccess to provide remote oversight for corporate laptops as though the devices were on the internal network.

HOTPin gives administrators the flexibility they need through the wide range of connectivity options that include clients for smart devices, SMS text messaging, and a PC desktop client. By leveraging smart devices or text messaging, the OTP is delivered 'on demand' to the user. And, of course, HOTPin easily integrates with AD.

Security for IT and users

DirectAccess with HOTPin is actually a security tool masquerading as a user convenience tool, a functional duality that, in other solutions, usually results in a trade-off.

Contact

USA +1 (510) 668-0700
UK +44 (0) 1189 596198
Singapore +65 6781 0700
India +91 98 208 90884
Japan +81 (0) 3-5210-2991

www.celestix.com
info@celestix.com

Conclusion

In an ever-changing technology environment, it is difficult for companies to determine which technologies will produce operating benefits and competitive advantage. Too often more security means that employees are unable to work effectively; worse, easy access results in compromised security that risks intrusion or data theft.

The Celestix WSA appliance can deliver DirectAccess, UAG and HOTPin, the solution trinity of simplified deployment, use and management. The WSA delivers Microsoft's vision for efficient, secure computing. Your employees will be able to work without navigating complex technology, and IT shouldn't compromise corporate security or integrity to accommodate a user's limited technical capacity.

Choice is a not a compromise.