celestix

Security Considerations for DirectAccess Deployments

Whitepaper

February 2015

Security, Simplified.

Overview

This white paper discusses security planning for DirectAccess deployment.

Introduction

DirectAccess represents a paradigm shift for remote access.

What is DirectAccess

Technology to provide secure, seamless, always on remote network connectivity.

DirectAccess Authentication

Tunnel infrastructure leverages IPsec.

DirectAccess Network Configuration

Leverage edge security to reduce exposure.

Advanced DirectAccess Security Configuration

Employ strong authentication.

Comparing DirectAccess to Client-Based VPN

Security benefits and limitations.

Split Tunneling vs. Force Tunneling

Tunnel connection benefits and limitations.

Lost or Stolen DirectAccess Devices

Mitigated risk for missing devices.

Security and the Celestix E Series Appliance

Stronger security, simpler deployment.

Conclusion

The Celestix E Series helps you to better manage your remote access solution.

Introduction

Microsoft DirectAccess is a remote access technology included as part of the Unified Remote Access role in Windows Server 2012 R2. It represents a paradigm shift in the way remote access is provided to corporate-managed Windows devices. DirectAccess is fundamentally built using existing, widely deployed industry standard protocols for which security configuration is will understood. However, many organizations want to better understand the specific security features incorporated with DirectAccess.

This whitepaper serves to provide an overview of security features in DirectAccess. It will explain in detail how the authentication process works, provide insight in to optional security configurations, compare DirectAccess with traditional client-based VPN, explore the differences between split and force tunneling, and outline how to address lost or stolen DirectAccess devices. Finally the benefits of using the Celestix E Series hardware appliance platform and its additional features and enhancements can provide the best experience for DirectAccess deployments.

What is DirectAccess

DirectAccess is a collection of Windows platform technologies that are assembled to provide secure, seamless and transparent, always on, bi-directional network connectivity for remote Windows machines. DirectAccess leverages authenticated IPsec encryption for integrity and confidentiality, and IPv6 for transport. IPv6 transition and translation protocols are used to ensure full compatibility with IPv4 networks and hosts. Authentication occurs at several stages and utilizes a combination of digital certificates, NTLM, and Kerberos. Windows Firewall with Advanced Security (WFAS) connection security rules on the client are used to establish DirectAccess communication, and DirectAccess configuration for both the client and the server are distributed via Active Directory group policy.

DirectAccess Authentication

When a DirectAccess client is outside of the corporate network and has an active Internet connection, the client will attempt to establish connectivity with the DirectAccess gateway by creating IPsec tunnels defined by the connection security rules in the Windows Firewall on the client. In a typical configuration, two distinct DirectAccess tunnels are established – an infrastructure tunnel and an intranet tunnel.

- **Infrastructure tunnel** – This IPsec tunnel provides secure remote network access to limited internal resources. Specifically, only infrastructure services such as domain controllers and systems management servers are available over this first tunnel. The infrastructure IPsec tunnel requires two forms of authentication. First, the client machine is authenticated using a computer certificate issued by the corporate Public Key Infrastructure (PKI). Second, the client machine's computer account is also authenticated against Active Directory using NTLM. If the client successfully passes both authentication steps, the infrastructure IPsec tunnel is established and the client can access infrastructure resources defined by the remote access policy. This IPsec tunnel uses 192 bit AES encryption and SHA-1 for integrity.

- **Intranet tunnel** – This IPsec tunnel provides the end user with full access to the corporate network. It is initiated when the users logs on to the DirectAccess client. The intranet tunnel also requires two forms of authentication. First, the computer is authenticated once again using the computer certificated issued by the corporate PKI. Second, the user account is authenticated against Active Directory using Kerberos. If the client successfully passes both authentication steps, the intranet IPsec tunnel is established. Like the infrastructure tunnel, this IPsec tunnel also uses 192 bit AES encryption and SHA-1 for integrity.

DirectAccess Network Configuration

DirectAccess in Windows Server 2012 R2 can now be configured behind an existing edge firewall for additional protection. Using this deployment model, the DirectAccess server is configured using private IPv4 addresses. The server can be configured with two network interfaces in parallel with existing perimeter networks, or with a single network interface either in the DMZ or on the LAN.

Perimeter/DMZ deployments reduce the exposure of the DirectAccess server to untrusted networks. This improves security, but can negatively impact scalability and performance when Windows 7 clients are supported. When the DirectAccess server is located behind a device performing NAT, it supports only the IP-HTTPS IPv6 transition protocol for DirectAccess clients. IP-HTTPS uses SSL/TLS to encrypt DirectAccess communication which is already encrypted using IPsec. This double encryption results in high protocol overhead that introduces latency and increases resource utilization on both the client and the server.

Advanced DirectAccess Security Configuration

To provide even higher levels of assurance for DirectAccess clients, strong user authentication can be implemented using smart cards (physical or virtual), RSA SecurID tokens, or One-Time Password (OTP). Custom configuration can be employed to provide additional security. For example, with additional configuration, DirectAccess clients can perform more stringent validation checks when establishing DirectAccess IPsec tunnels, ensuring that DirectAccess clients will only establish a connection with a DirectAccess server with a specific tunnel endpoint IPv6 address and that includes a certificate that uses a custom Object Identifier (OID).

To further enhance the overall security of DirectAccess, a third-party Application Delivery Controller (ADC) can be deployed to provide a level of pre authentication for DirectAccess clients. Also, encryption methods using stronger cipher suites and Perfect Forward Secrecy (PFS) can be configured.

Comparing DirectAccess to Client-Based VPN

DirectAccess provides a much higher level of security when compared to traditional client-based VPN. The supporting infrastructure requirements make the solution inherently more resistant to unauthorized access.

For attackers to compromise a DirectAccess connection, they would require a computer that is a member of the organization's Active Directory domain, and the computer account would need to belong to the defined DirectAccess security group. In addition, a computer certificate issued by the company's internal Public Key Infrastructure (PKI) is required. The attacker would also require valid user credentials to access corporate resources.

To compromise a client-based VPN connection, an attacker would only require a VPN client, which is included in the operating system or readily available. Since the attacker can mount the attack from any system, the risk of compromise through this channel is great. Multifactor authentication can mitigate this risk for both VPN and DirectAccess, however.

Both solutions share similar potential risks. The remote access server can be discovered via common reconnaissance methods and user credentials obtained surreptitiously. However, the DirectAccess connection is more resistant to compromise because the attack cannot be carried out from just any machine. For an attacker to successfully spoof both an AD computer account and computer certificate is extremely difficult. And if successful, the attacker has likely already compromised the target organization.

Split Tunneling vs. Force Tunneling

By default, DirectAccess is configured with split tunneling enabled. This allows the DirectAccess client to connect to the public Internet and the corporate network simultaneously. Some security administrators believe this to be a security risk, but closer evaluation reveals this risk to be more perceived than actual.

One concern with split tunneling is that a compromised device could allow an attacker to tunnel from the Internet through the connected DirectAccess client to access resources on the corporate network. However, the authenticated nature of the DirectAccess IPsec tunnels makes this impossible.

If a DirectAccess client is infected with a virus or malicious software, it may be possible for it to infect other hosts on the corporate network via the DirectAccess connection. However, this scenario also applies to traditional VPN clients. The risk is reduced with DirectAccess because they are always managed, and this maintenance of client security posture allows for better malware defense and client protection.

With split tunneling, DirectAccess clients have unrestricted access to the public Internet. This lack of filtering is a valid concern for security administrators, but again, this problem exists for traditional VPN clients too. A VPN client with split tunneling disabled may not be able to access the Internet freely while connected to the VPN, but once the user disconnects the VPN session they will once again has full unrestricted Internet access.

There are several ways to mitigate this issue. DirectAccess can be configured to enable force tunneling, which requires DirectAccess clients to use the on-premises corporate proxy servers to access the Internet. Force tunneling has some potential negative side effects, however. By forcing all of the client’s Internet traffic over the DirectAccess connection, the user experience is often degraded by additional network latency introduced by encryption and web proxy traffic inspection. Also, the added network load can degrade performance and limit scalability of the DirectAccess server.

A better solution is to enable remote filtering on existing on-premises secure web gateways (if available) or to investigate the use of cloud-based web content filtering solutions for mobile clients.

Lost or Stolen DirectAccess Devices

Concerns that always-on DirectAccess clients represent an increased security risk are unfounded. Like a device configured for client-based VPN, an attacker would need valid user credentials to gain access to the network, but DirectAccess includes additional safeguards. Clients use computer accounts that can be disabled in Active Directory to prevent connectivity, even if valid user credentials are supplied. If real-time remediation is necessary, terminating an active client session forces authentication, which will fail after the computer account is disabled.

The DirectAccess client presents the same risks as a client configured with client-based VPN. Many of these risks can be mitigated using a combination of operational security techniques and technologies commonly used today. Mobile clients should be configured with full disk encryption and require a PIN to boot the device. They should be configured to require a password to be entered when waking from sleep or hibernation. Strong user authentication using smart cards or dynamic passwords can also be leveraged.

Security and the Celestix E Series Appliance

The DirectAccess solution is improved by additional security measures included with the Celestix E Series appliance platform. Based on Microsoft and industry standard security best practices, the E Series has undergone extensive hardening and attack surface reduction. These processes disable or remove unnecessary services, applications, roles, and features for a stronger security posture. Additional measures include updating the default configuration of the Windows firewall to further restrict remote access to services running on the host and improving default encryption algorithms used by applications and services.

While augmenting the security, the E Series also offers simplified deployment and centralized management features. The platform lowers the total cost of ownership and maintenance overhead presented in other deployment options.

Conclusion

DirectAccess is a compelling remote access solution that can be used to better manage remote Windows clients and dramatically improve their security posture, while at the same time securely providing ubiquitous and familiar remote access to on-premises applications and data. DirectAccess leverages mature, well understood, and commonly deployed Windows platform technologies. Client connections are fully authenticated using a combination of digital certificates, in addition to machine and user authentication. The solution provides significantly higher levels of assurance when compared to traditional VPN, and security can be further enhanced with custom configuration. DirectAccess provides support for both split and force tunneling, and lost or stolen devices can be denied remote access administratively. The Celestix E Series hardware appliance platform increases the solution’s security through service hardening and attack surface reduction, and simplifies feature installation with streamlined management interface.

Contact

Celestix Networks, Inc.

3215 Skyway Ct.
Fremont, California 94539

www.celestix.com
sales@celestix.com

510.668.0700

facebook.com/celestixnetworks
twitter.com/CelestixNetwork