E Series FAQ: DirectAccess Feature

Q: What is DirectAcces (DA)?

A: DirectAccess provides seamless and transparent, always on, bi-directional remote network connectivity for managed Windows clients. Administrators can manage clients when they are outside the network, and remote users can access internal network resources whenever they have an Internet connection.

Q: What's the difference between DirectAccess and VPN?

A: DA and traditional VPN's both allow remote access to the internal network, but DA also allows remote management to maintain client compliance with security policies. Also, client-based VPN requires the user to initiate a connection to the corporate network where DirectAccess does not.

Q: What are the requirements to deploy DirectAccess?

A: The minimum DA infrastructure requires:

- Server running Windows Server 2012 R2 for current full functionality
- Active Directory
- DNS
- Clients and servers must be domain joined
- Public key infrastructure (PKI) is required to support Windows 7 clients, in addition to advanced features like OTP authentication, NAP integration, and multi-site deployments.

Required certificate:

- SSL certificate – an SSL certificate issued from a trusted third-party public CA is recommended, but an internal CA can be used. If an internal CA is used, the certificate revocation list (CRL) must be publicly available.

Recommended:

- Computer certificate – a computer certificate issued to the DirectAccess server and clients from internal CA.

Q: How do I determine hardware needs?

A: It's recommended to run DA on its own hardware, with supporting technologies running on separate servers. Each deployment will have its own needs for hardware components.

Q: What clients are supported?

A: Windows 7 Enterprise and Ultimate, Windows 8 and later Enterprise.

Q: What if I need external access for devices that aren't supported?

A: The Remote Access role in Windows Server 2012 includes a client-based VPN option that supports PPTP, L2TP/IPsec, SSTP, and IKEv2 protocols.

Q: How many clients can a DirectAccess server handle?

A: Celestix E Series appliances can handle between 500 and 5000 concurrent users.

Q: Is high availability (HA) necessary?

A: No it isn’t, but every environment is different, and some organizations may have policies or other requirements that would necessitate an HA deployment. The E Series solution supports load balancing (integrated and external) for local high availability and redundancy. In addition, a multisite configuration option is available to provide geographic redundancy

Q: What encryption does DirectAccess use?

A: Advanced Encryption Standard (AES)

Q: Can I virtualize a DirectAccess deployment?

A: Yes, but as DA is fairly resource intensive, it's almost always better to deploy on a dedicated appliance.

Q: How does my IPv4 network handle the IPv6 requirements?

A: As long as IPv6 is enabled for the network adapter(s) that handle DA communication, the necessary translation happens automatically.