F5 and Windows Server 2012 DirectAccess/Remote Access Services

The F5 BIG-IP platform provides high availability, performance, and scalability when used to deliver traffic management and load balancing for the Microsoft Windows Server 2012 Remote Access Solutions: DirectAccess and Remote Access Services.

White Paper

by Ryan Korock

Introduction

For Windows 8 and Windows Server 2012, Microsoft has taken two remote access technologies found in previous versions of Windows Server, DirectAccess and VPN Server, and pulled them under the same management umbrella called simply Remote Access. F5 technologies can be deployed to manage traffic and balance loads on these services.

Originally introduced in Windows Server 2008 R2 and Windows 7, DirectAccess shifted previous remote access technology. Unlike traditional VPNs, in which connections have been manually initiated at the user level, DirectAccess makes use of a seamless, system-level connection. This means that remote, domain-joined systems will automatically and securely build a corporate network presence upon boot.

VPN, formerly known as Remote Access Services (RAS), was introduced in Windows NT and includes the traditional Windows VPN technologies, including IKEv2, SSTP, PPTP, and L2TP. Windows Server 2012 customers can deploy DirectAccess, VPN, or both, and it is often beneficial to deploy both. DirectAccess provides remote access for domain-joined Windows 7 (and greater) clients who have been granted the proper permissions, while VPN offers remote access to those machines that are not domain-joined or not yet running Windows 7.

New to DirectAccess in Windows Server 2012 is support for both local and wide area load balancing. F5 BIG-IP Local Traffic Manager (LTM) can be used to provide local area load balancing, and F5 BIG-IP Global Traffic Manager (GTM) can provide the wide area (a.k.a. global) load balancing.

Benefits of Using F5 Products with DirectAccess and VPN

F5 products can play a significant role in a Windows Server 2012 Remote Access deployment.

- **High Availability** Through awareness of the actual DirectAccess/VPN services, BIG-IP LTM can ensure users are always sent to a DirectAccess/VPN server that is ready for new connections, eliminating situations in which a user is sent to a down or poorly performing server. In addition, BIG-IP LTM features persistence functionality across services. This is advantageous when handling traffic such as point-to-point tunneling protocol (PPTP), which has shipped with every version of Windows client since Windows 95 R2, giving it incredibly wide coverage on client computers. Each client connecting to DirectAccess via PPTP creates two independent but required flows-the control connection and the data connection-and when load balancing, both flows from each client must be sent to the same PPTP server to avoid breaking the connection. BIG-IP LTM has the intelligence to send both flows from a particular client to the same server, thus ensuring the connection remains unbroken.
- **Scalability** By intelligently managing traffic, BIG-IP LTM can distribute throughput to a multisite farm of DirectAccess/VPN servers, allowing the system to scale to a far greater number of users than it could otherwise handle.
- **Performance** BIG-IP LTM can help with performance in a variety of ways, from TCP optimizations and SSL offloading to server performance awareness. The result is faster access and the best possible network experience for users. In particular, BIG-IP LTM SSL/TLS encryption offloading can relieve the DirectAccess/VPN servers of large workloads. By terminating the SSL connection with the client and sending the traffic unencrypted to the servers, BIG-IP LTM frees server CPU for serving clients.
- **Security** The same BIG-IP LTM device providing traffic management for the DirectAccess/VPN servers is an ICSA Certified network firewall, meeting the data center security standards that allow enterprises to deploy it as a dual use Application Delivery Controller (ADC) and perimeter security appliance.

Architecture

Careful consideration of the proper network architecture for DirectAccess/VPN is a critical step in the deployment process. Many options and topologies can be used, and what's here is not intended to be an exhaustive list addressing all deployments, but merely a review of the main decision criteria and a few recommended topologies. Criteria that commonly affect deployment topologies include scale, security requirements, budgets, and service level agreements (SLAs). Since these considerations often drive a certain architecture or prohibit others, it is best to consult with F5 and Microsoft teams before deployment.

For high availability, F5 strongly recommends deployment of BIG-IP LTM appliances using either an active/standby deployment model or a group of two or more devices actively supporting each other, which may be referred to as an activeN model. Both of these models allow for a BIG-IP LTM failover without any disruption to network connections. In the following diagrams, a single BIG-IP LTM icon represents a failover pair or activeN group.

A DirectAccess/VPN Server Front End

To provide application delivery and load balancing for DirectAccess, organizations often deploy BIG-IP LTM in front of their DirectAccess/VPN servers as a formal front end. Among other things, this BIG-IP device becomes responsible for monitoring the DirectAccess/VPN services for availability and distributing incoming client connections to the servers.

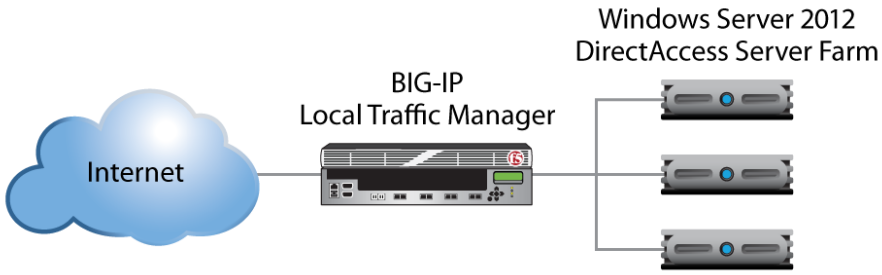

Figure 1: BIG-IP LTM as the front end to a DirectAccess system

Windows Server 2012 DirectAccess Server Farm

A Layered Approach with DirectAccess/VPN Servers

Although not required for simple DirectAccess/VPN load balancing, placing BIG-IP LTM devices between the DirectAccess farm and the corporate network also offers significant benefits. Specifically, this configuration enables a "manage out" scenario in which clients or servers on the internal network can initiate management connections to the remotely connected DirectAccess clients. In addition, internal farms of application servers can be load balanced and subjected to other useful traffic management operations.

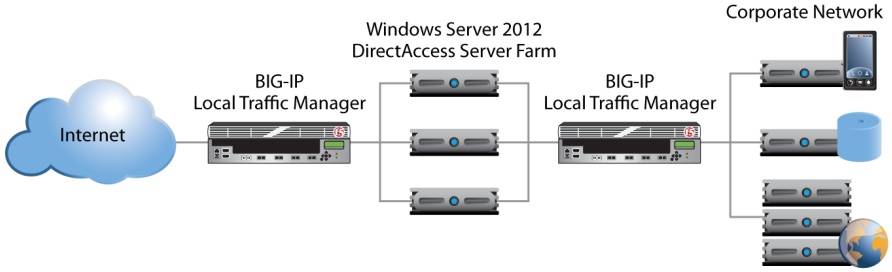

Figure 2: External and internal BIG-IP LTM devices in a layered approach

Dual vs. single (paired) BIG-IP LTM device deployments

Having a BIG-IP LTM device in front of the DirectAccess/VPN farm is considered a requirement for optimal availability, and another device on the corporate network side of the farm is highly recommended. This doesn't necessarily require separate BIG-IP LTM devices. The layered model can be easily deployed by reusing the same BIG-IP LTM device for both external and internal roles. See Figure 3.

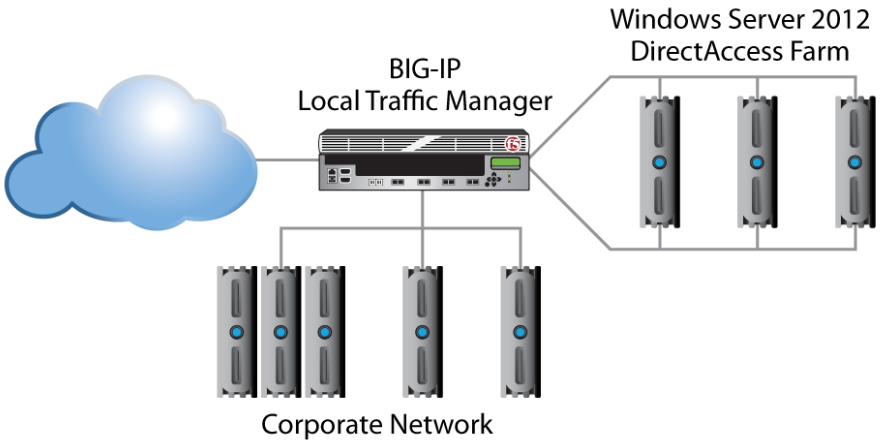

Figure 3: A single BIG-IP LTM device in a layered deployment

Windows Server 2012 DirectAccess Farm BIG-IP Corporate Network

Dual Interface Vs. Single Interface DirectAccess/VPN Deployments

In addition to selecting a front-end or layered approach, organizations must also choose whether to deploy their Direct Access/VPN servers with a dual homed/ networked interface or a single network interface controller (NIC).

Dual interface deployment

DirectAccess supports a dual interface routed configuration that segments the external network from the corporate network. This configuration provides for a segmented deployment and is required for use of the Teredo access protocols available in the DirectAccess suite. Designed to be lightweight and secure, the Teredo protocol is network address translation (NAT) friendly.

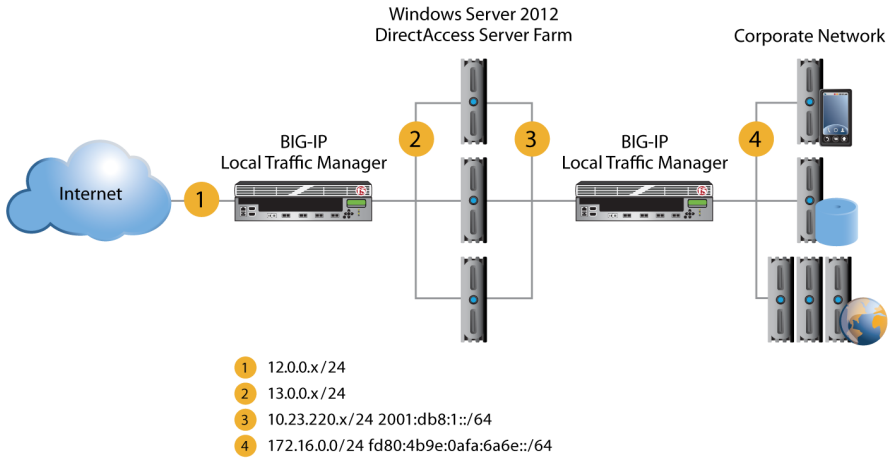

Figure 4: A layered deployment with dual interface routing

Single interface deployment

DirectAccess also supports single interface deployment models in which each DirectAccess server has only one NIC. Corporate Network

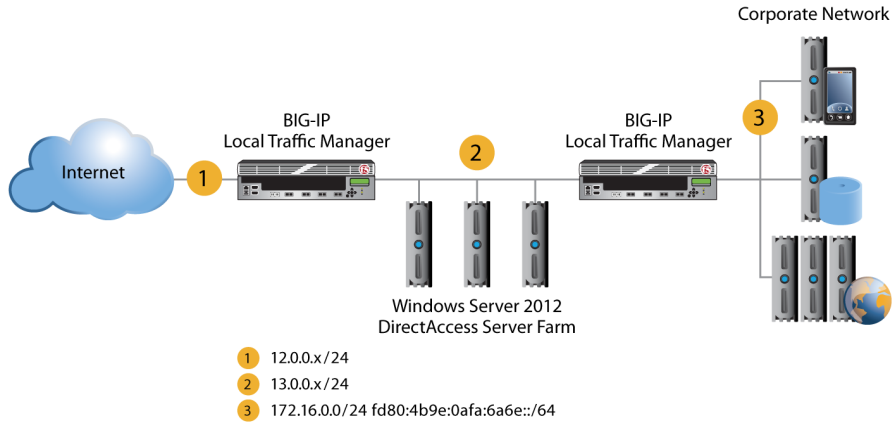

Figure 5: A single interface deployment with dual BIG-IP LTM devices

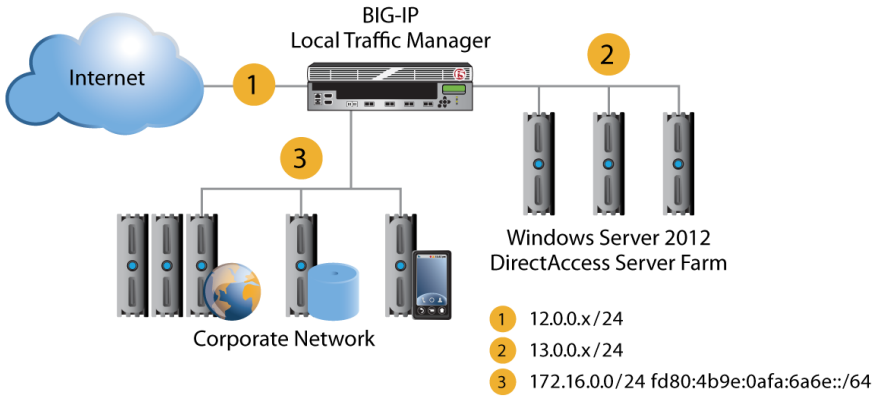

Figure 6: A single interface deployment with BIG-IP LTM in a layered configuration

Single Site Vs. Multisite Deployment

Deployments with large, multi-national user bases or requirements for site level resiliency may opt to go with a multi-site deployment. In such a scenario, F5 BIG-IP GTM can be deployed in addition to BIG-IP LTM to provide wide-area traffic management and context-aware load balancing.

BIG-IP GTM is a global traffic management device that extends the benefits of the BIG-IP platform by monitoring site-level health, handling traffic (including remote client requests) coming from outside of the site, and providing site-level disaster recovery capabilities. Among the capabilities of BIG-IP GTM are geographic awareness and the direction of remote users to the geographically closest DirectAccess farm. BIG-IP GTM also ensures site-level failover to active data center(s) when planned or unplanned outages occur.

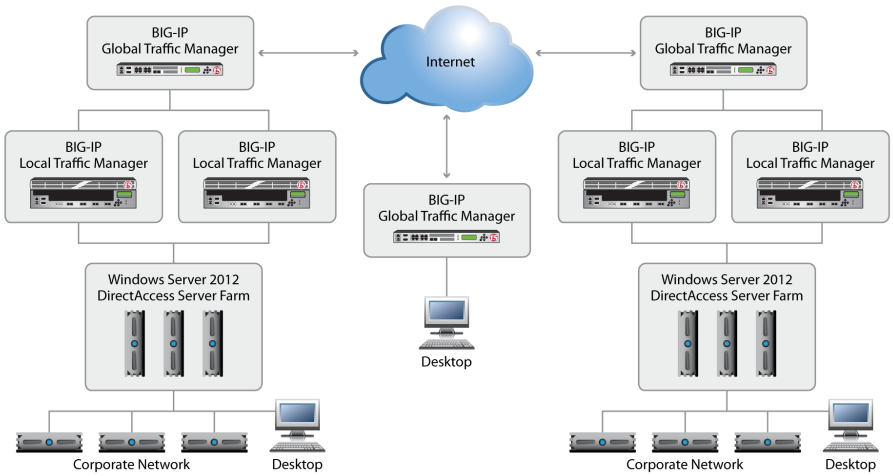

Figure 7: A wide area DirectAccess/VPN deployment

Conclusion

Regardless of the configuration topology best suited to an organization's architecture and needs, F5 products can play a significant role in a Windows Server 2012 DirectAccess/VPN deployment. BIG-IP LTM and BIG-IP GTM can work together to provide both server and site level resiliency for DirectAccess and Remote Access Services. By intelligently managing traffic with service, context, and user awareness; service persistence; and unmatched throughput capabilities, the BIG-IP platform maximizes availability and ensures scalability. Sophisticated, hardware-based optimization technologies and offloading of encryption/decryption increase system performance and server capacity while improving the user experience. An ICSA Certified network firewall as well as an ADC, BIG-IP LTM also performs as a perimeter security device and can be further enhanced with other policy management and security modules of the BIG-IP family. By deploying BIG-IP products with DirectAccess/VPN, organizations can maximize the overall benefits and security of their remote access investments.

F5 Networks, Inc.
401 Elliott Avenue West, Seattle, WA 98119
888-882-4447 www.f5.com

Americas
info@f5.com

Asia-Pacific
apacinfo@f5.com

Europe/Middle-East/Africa
emeainfo@f5.com

Japan
f5j-info@f5.com