v10.1 - BIG-IP and Microsoft DirectAccess

Joe Pruitt, 2009-18-11

For the enterprise user, Windows 7 adds a slew of new features in it's Enterprise edition including BranchCache, Federated Search, AppLocker, BitLocker, as well as the focus of this article: DirectAccess.

So What Is DirectAccess?

DirectAccess in Windows 7 and Windows Server 2008 R2 allows users to seemlessly and securely connect to their corporate network without the need to establish a separate VPN connection. With a DirectAccess enabled environment, the network's file shares, applications, and intranet are accessible whenever and whereever you have an Internet connection.

Implemented as an IPv6 over IPSec tunnel, all network access is encrypted when it travels across public networks. Leveraging IPSec, PKI, and Active Directory, DirectAccess can authenticate both the computer and the user. It additionally adds supports multifactor authentication such as a smart card.

For network administrators, having a transparent connection to their remote machines whenever they have network connectivity means that they can schedule service updates on a regular basis and ensure that mobule users stay up to date with company policies.

BIG-IP Integrates With DirectAccess

The BIG-IP Local Traffic Manager will be used to provide scalability and high availability for a Microsoft DataAccess deployment. As illustrated in this diagram, BIG-IP can function for internal and external clients.
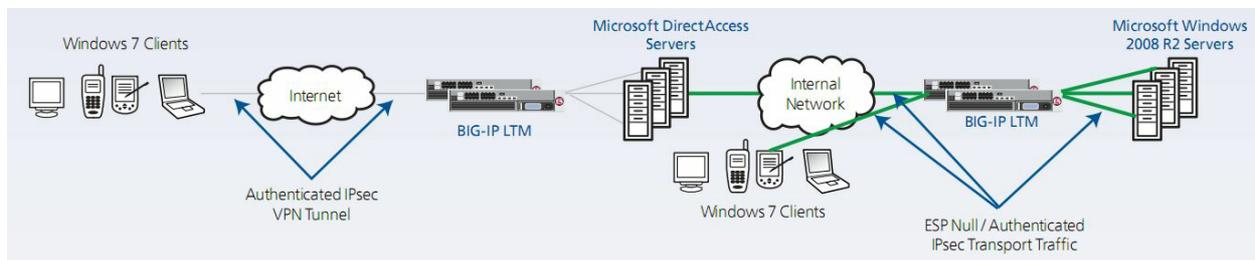
The BIG-IP system's load balancing capabilities are designed to route both incoming and outgoing traffic through the most appropriate path. Once a user has authenticated and established an encrypted tunnel with the DirectAccess server, instead of connecting directly to the application server in a typical DirectAccess deployment, BIG-IP LTM sits inline and proxies those connections to ensure users get either the most available server (for a new connection) or the most appropriate server (for established 'sticky' sessions) for that request.

Benefits Of The BIG-IP LTM/DirectAccess Solution

- Reliability
- Accelerated Applications
- Reduced Server And Bandwidth Cost
- Greater Network and Application Security
- Unmatched Application Intelligence And Control
- Total Integration For All IP Applications
- Industry-Leading Performance
- Easy To Manage, Better Visibility

Implementing Connection Tracking

The following iRule can be used to implement the connection tracking for DirectAccess server request.

```
when SERVER_DATA {
  set session_key [IP::local_addr]
  session add uie [$session_key any virtual] [LINK::nexthop] 43200
```

```
    session add ule {$session_key any virtual} [LINK::nexthop] 43200
    log local0. "Session table entry added for $session_key to [LINK::nexthop]"
  }
```

The connection tracking iRule records the source IP address of the connection and the MAC address of the sending DirectAccess server into an internal table on the BIG-IP. This information is used later ot make sure that a connection to the same client is always sent to the same DirectAccess server. To create this iRule:

1. Log into the BIG-IP Administration GUI.
2. On the Main tab, expand Local Traffic, and then click iRules. The iRules screen appears.
3. In the upper right portion of the screen, click the Create button. The New iRule screen appears.
4. In the Name box, enter a name for your iRule (ie. DirectAccessPersistence).
5. In the Definition section copy and paste the above iRule.
6. Click Finished.

Implementing Direct Access with Microsoft Forefront Unified Access Gateway (UAG)

Unified Access Gateway extends the Direct Access solution by integrating a sophisticated management interface as well as adding control over multiple access protocols. For those of you looking to implement UAG, F5 has created a landing page for that technology here. We've also developed a deployment guide for BIG-IP LTM & UAG here, that discusses the finer points of leveraging BIG-IP for scaling UAG.

Resources

- Microsoft Server And Tools: DirectAccess
- Microsoft Windows Enterprise: Windows 7 Features