# Connecting to Windows Azure with the BIG-IP

Updated 3 years agoOriginally posted March 22, 2013 by [**Greg Coward**](https://devcentral.f5.com/s/profile/0051T000008uGkxQAE)[F5](https://devcentral.f5.com/s/profile/0051T000008uGkxQAE)

Topics in this Article: [application delivery](https://devcentral.f5.com/s/articles?tag=Application%20Delivery), [azure](https://devcentral.f5.com/s/articles?tag=Azure), [cloud](https://devcentral.f5.com/s/articles?tag=Cloud), [ltm](https://devcentral.f5.com/s/articles?tag=LTM), [us](https://devcentral.f5.com/s/articles?tag=us)

**“Everybody’s going to the cloud! Everybody’s going to the Cloud!”**

<https://devcentral.f5.com/s/articles/connecting-to-windows-azure-with-the-big-ip>

Well…alright….not exactly. While organizations of varying sizes are utilizing cloud resources with increasing frequency, the majority have definitely not gone “all-in”. Still, with the increasing popularity of cloud-based services like Office 365 and Windows Azure, the pace of adoption appears to be picking up and many adopters are starting to move their services up to the cloud. In a few of my previous [posts](https://devcentral.f5.com/blogs/us/big-ip-and-adfs-part-2-ndash-ldquoapm-ndashan-alternative-to-the-adfs-proxy-rdquo), we talked about how the [F5 BIG-IP](http://www.f5.com/) can enhance the sign-on experience between an organization’s on-premise Active Directory and Office 365. So, it only seems fitting to take a look at how F5 and the BIG-IP can facilitate the Windows Azure experience.

One of the many features of Windows Azure is its “Virtual Network” functionality which allows organizations to provision and manage cloud-based virtual private networks. These virtual networks can host a variety of resources such as webservers, databases, etc. that have been traditionally hosted in the on-premise data center. What’s more, by utilizing a ‘site-to-site’ VPN between the on-premise network and the virtual network(s), the on-premise data center can now be scaled-out quickly and easily. For example, in the scenario below rather than investing in additional on-premise infrastructure, the organization, (F5Demo) has decided to use Windows Azure to host both its SharePoint and [AD FS farms](https://devcentral.f5.com/blogs/us/big-ip-and-adfs-part-1-ndash-ldquoload-balancing-the-adfs-farm-rdquo). Along with load balancing and providing pre-authentication for both on-premise and cloud-based [applications](http://www.f5.com/products/documentation/deployment-guides/), the BIG-IP can act as the [IPsec gateway device](http://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos-implementations-11-3-0/17.html?sr=26371865) for establishing a secure ‘site-to-site’ VPN with Windows Azure.

F,{65a91dcb-142e-4e18-85fb-1f0a8a0139df}{114},3.125,3.125

Rather than providing step-by-step guidance on configuring IPsec on the BIG-IP, I’m just going to provide a brief overview of the steps required. However, don’t fret! There’s an iApp for it! Yep just click [here](https://devcentral.f5.com/s/articles/ipsec-tunnel-endpoint-iapp-949) and download the iApp template. **Please Note:** Although I have configured and tested the template, it is offered under the community submitted category and subsequently, not F5 supported. In addition, there’s great guidance for configuring the BIG-IP available on [F5’s support site](http://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos-implementations-11-3-0/17.html?sr=26371865). Additionally, information regarding Windows Azure IPsec requirements can be found [here](http://msdn.microsoft.com/en-us/library/windowsazure/jj156007.aspx). Configuring the BIG-IP as an IPsec tunnel endpoint is relatively simple and consists of four, (4) steps.

|  |  |
| --- | --- |
| ***Step1.*** *Create an IKE peer –* The Azure IKE peer, (Phase I) utilizes ‘*SHA-1*’ for authentication, ‘*AES128’* for encryption, Diffie-Hellman (MODP1024) Perfect Forward Secrecy, and a ‘*preshared key’.*  F,{65a91dcb-142e-4e18-85fb-1f0a8a0139df}{152},3.125,3.125 | ***Step2.*** *Create an IPsec policy* – The IPsec policy, (Phase II) utilizes *SHA-1*’ for authentication, ‘*AES128’* for encryption, and Diffie-Hellman (MODP1024) Perfect Forward Secrecy.  F,{65a91dcb-142e-4e18-85fb-1f0a8a0139df}{164},3.125,3.125    **Note:** *The local endpoint, (BIG-IP) must use a publicly routable IP address as its tunnel endpoint.* |
| ***Step3.*** *Create Traffic Selector(s)* - The traffic selectors specify what traffic, (based on source and destination addresses) to pass through the IPsec tunnel.  F,{65a91dcb-142e-4e18-85fb-1f0a8a0139df}{188},3.125,3.125 | ***Step4.*** *Create a forwarding virtual server –* The simple forwarding virtual server listens for and directs traffic over the IPsec tunnel.  F,{65a91dcb-142e-4e18-85fb-1f0a8a0139df}{200},3.125,3.125 |

There you have it! It’s as easy as 1, 2, 3,…ah....4. Once again, I didn’t want to reinvent the wheel so checkout the [F5 support page](http://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos-implementations-11-3-0/17.html?sr=26371865http://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos-implementations-11-3-0/17.html?sr=26371865) for detailed guidance on configuring the BIG-IP and IPsec.

***Additional Links:***

[***Codeshare - IPSec Tunnel Endpoint iApp***](https://devcentral.f5.com/s/articles/ipsec-tunnel-endpoint-iapp-949)

[***Configuring IPsec between a BIG-IP system and a third-party device***](http://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos-implementations-11-3-0/17.html?sr=26371865http://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos-implementations-11-3-0/17.html?sr=26371865)

[***Windows Azure Virtual Networks***](http://msdn.microsoft.com/en-us/library/windowsazure/jj156007.aspx)