v.10 - Introduction to iSessions

Don MacVittie, 2009-29-04

Amongst the wave of new features that came out in Version 10 of TMOS is a nifty little feature called iSessions. This being the first release of iSessions, there is a lot of curiosity and not as much documentation as we'd like yet. So I'll walk you through what is available, why you'd want to use it, and what benefits it offers in this blog post. As time goes on we will expand our coverage of iSessions to more fully discuss all of the options and challenges they present.

The concept of iSessions in v.10 is pretty straight-forward… A secure tunnel between two BIG-IP systems to share in load-balancing and failover. The extension is that those BIG-IPs can be (and generally should be) geographically remote. Indeed, the whole point of iSessions is to make WAN communications faster, but we've got enough experience to know that some of you will find a use for them inside the datacenter. iSessions only require that the BIG-IPs be able to route between each other, not that they be geographically remote. Since optimization of traffic over an iSessions link is built in, you get both secure and accelerated WAN communications. The type of optimization is configurable, as are several other things about the tunnels.

While this post isn't intended to be a step-by-step How-To document, it will give you an overview of the steps necessary to get your BIG-IPs talking on the "back channel", and offer some points of interest for you to be aware of.

Much like some vendors have a remote office solution that is simply an optimizing proxy for their data center products, iSessions will forward requests to a remote BIG-IP. Unlike those solutions, if the connection the iSessions communicate over is down, the BIG-IP can be configured to handle the request locally if you have the servers in-place.

For this blog post we will refer to the "Data Center BIG-IP" and the "Remote BIG-IP" note that the "Remote BIG-IP" could be configured in an alternate data center, and thus could be fulfilling both the role of the Data Center BIG-IP in some instances and that of the Remote BIG-IP in others. For simplicity's sake, we will not explore that configuration here, simply note that it's possible. For this blog post, the "Remote BIG-IP" is the device that the user's requests will come in through, the "Data Center BIG-IP" is the one that will ultimately service requests.

That should be all the background we need to cover, now on with the overview.

The best way to think of iSessions (for me at least) is like a fibre optic cable. iSessions are turned on at both Remote and Data Center BIG-IPs, and that creates the sheath that holds the fibres. When connections are requested on the Remote BIG-IP, an individual fiber (connection) is created in the sheath (tunnel). Depending upon your settings, that connection could exist for a long time, servicing repeated requests from different clients, or it could exist only so long as the requesting connection is live.

At its simplest, the iSessions configuration is easy. On the Remote BIG-IP, you configure a forwarding Virtual Server to forward requests to the Data Center BIG-IP. The Data Center BIG-IP has a Virtual Server configured for iSessions that either maps to a server or forwards to another Virtual Server on the same BIG-IP. Either way, the Data Center BIG-IP services the request, and sends the response along the same iSession connection, assuming the request is for the same target Virtual Server. Note that re-use has some drawbacks in every implementation out there, and you might want to consider their use carefully if you have very bursty traffic patterns. Also note that in this first implementation of iSessions, the longevity of a connection is 10 minutes and cannot be changed.

Note that the iSession Forwarding Virtual Server is different than most Forwarding Virtual Servers – it is configured as a standard Virtual Server with address/port translation turned off and no Pool object associated with it. A destination is then set that is the Data Center BIG-IP's address. The Virtual Server on the Remote BIG-IP requires a TCP profile to be selected for both the client and server side contexts, and a client SSL profile must be selected so that iSessions info can be decrypted when the other BIG-IP sends responses.

This Virtual Server on the Remote BIG-IP also requires an iSession Profile to be selected so that tells the BIG-IP how to handle tunnel creation when communicating with the Data Center BIG-IP. The iSession profile specifically tells the BIG-IP about mappings to the Data Center BIG-IP, Session re-use, optimizations of the tunnel, and other general connection options like de-duplication (not currently available even if enabled… Check back for more info) and port transparency. Note that while the Endpoint Pool is slipped in at the bottom of the configuration screen, you need it set to a pool of one node that is the forwarding point for iSession Tunnels to the Data Center BIG-IP.

The Data Center BIG-IP has the same iSession Profile, and your choices for tunnel-specific configurations are compared when a tunnel is initiated, and only those settings that are enabled on both sides are used for this tunnel.

On the Data Center side, you must configure the iSession Profile such that it knows what to do with incoming connections – are they simply routed, or do they get sent to Virtual Servers for additional processing, etc. These options are at the bottom of the iSession Profile configuration. For Target Virtual type, your early implementations can probably use Match All, which will match to any Virtual that fits, and route the request on if none matches.

Okay, that's a ton of info. We'll call that the quick overview. The salient points are:

1. iSessions create an encrypted, optimized tunnel over the WAN between two BIG-IPs.
2. Both BIG-IPs must be v.10
3. When configuring client and server profiles remember to think of traffic direction… Where the traffic comes in from the client (regardless of which BIG-IP you're on) is the client side, where it flows back toward the client is the server side.
4. iSessions are always encrypted but you have options for which and how much compression to use (and the ability to choose "adaptive" if you are uncertain which is best for you).
5. Just because this blog post used "Remote BIG-IP" doesn't mean it can't also be in a data center, and in some instances it may even be the "Data Center BIG-IP" in highly distributed environments.
6. Session re-use saves the overhead of renegotiating for each connection, but comes with a price of long-lived connections between the two BIG-IPs.

That's it for now. I'll be posting soon about how and why this is important if you're considering using a cloud provider. Check with your SE if you're interested in more implementation-specific details.

Don.

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

F5 Networks, Inc.	F5 Networks	F5 Networks Ltd.	F5 Networks
Corporate Headquarters	Asia-Pacific	Europe/Middle-East/Africa	Japan K.K.
info@f5.com	apacinfo@f5.com	emeainfo@f5.com	f5j-info@f5.com