

Deploying BIG-IP with Tivoli Security Access Manager's WebSeal Proxy



Nojan Moshiri, 2013-12-06



Availability, it always comes back to this doesn't it? Sometimes a solution is so straightforward that I wonder if it deserves to be documented, but then I get a lot of phone calls and emails and my arm is twisted into publishing the solution. Not to downplay the significance of these solutions, because they mean a lot. If your authentication and entitlement system is not on-line, then neither are any of the applications protected by that system.

I am pleased to be able to share the results of testing and implementation of the load balancing solution for Security Access Manager. You can find the guide on [f5.com](http://www.f5.com):

<http://www.f5.com/pdf/deployment-guides/ibm-security-access-manager-dg.pdf>

We are looking at three basic components with this guide: configuring your WebSeal servers to be identical, configuring the Virtual Server and its components and finally, adding acceleration features if your WebSeal proxy is also serving content. Pretty straightforward, but the benefits are measurable in terms of uptime, increased performance on the servers and better user experience from the point of view of the users. Let's drill down into the details a bit, and then you can go try it for yourself via the deployment guide.

The first component in this solution is to make sure the WebSeal servers 1 through N are configured to be identical. This ensures that if a user is load balanced to any of the WebSeal servers that he or she will be able to be authorized and entitled to the same root. In other words, this step makes sure that authorization evaluations are identical on all the hosts.

Second, configuration of the BIG-IP is the fairly straightforward part of this solution. Nodes are created for each server, a pool is created for each member (node+port) and monitors, and profiles (TCP, HTTP and compression) are created and applied. One of the nicest features available in this solution comes in at this step. We recommend using step-down encryption methodology to maintain encryption while reducing the load on the WebSeal servers. By using 2k keys on the client side of the BIG-IP and 1k keys on the server side, the workload for the WebSeal server are more than halved. A big savings that reserves more CPU for the authorization and entitlement tasks at hand.

Finally, I was inspired to add the acceleration features to this document by my colleagues in Japan who rolled this out for a customer. By attaching a Web Acceleration profile, using the new Application Acceleration Manager (AAM - <http://www.f5.com/products/big-ip/big-ip-application-acceleration-manager/overview/>) we are able to see significant gains in user experience and reduction in server CPU and usage. You may be familiar with AAM if you previously used Web Accelerator.

I hope you enjoy the guide and provide your feedback..

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

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com