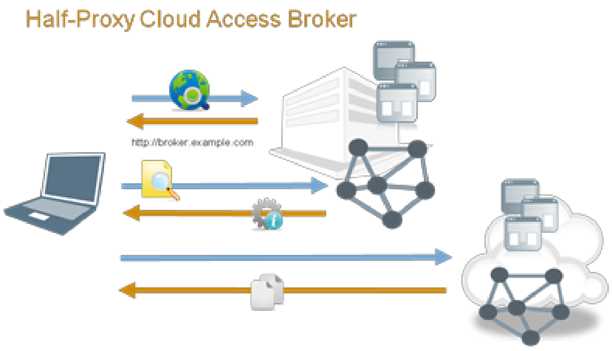
The Half-Proxy Cloud Access Broker

Lori MacVittie, 2012-11-06

#infosec #cloud #iam Though unfettered access to cloud-deployed applications is touted as a benefit, IT knows that control over access is necessary



That doesn’t mean that achieving that control is easy.

Well, maybe it’s easy than you might think.

The trick to managing access to cloud-deployed applications is requiring that access be brokered through infrastructure over which IT has control, i.e. through services IT can configure and manage itself to be compliant with corporate policies.

Doing so, especially given “anywhere, any client” access models, requires orchestration of several infrastructure components, starting with DNS.

DNS is (or should be) the gatekeeper to all corporate applications whether they’re deployed locally or in the cloud. By maintaining control over the corporate namespace, IT can ensure that requests for applications – regardless of from where those requests originate – can be managed in a manner consistent with corporate access policies.

Yes, users may want to use their iPad, but if it’s an unmanaged device and the application or resource being requested requires transfer of sensitive corporate data to the device, it may not be acceptable based on security policies (and a number of governmental regulations, as well). By controlling the namespace, IT can implement a first line of access control.

Once it’s been determined that the location is acceptable for the requested resource, DNS can return the appropriate resource to the user. That address is, of course, hosted locally and serviced by the application delivery tier, through which additional security measures can be executed to ensure appropriateness of access.

Such measures might include authentication processes – including additional security questions for verification of identity – as well as scanning the endpoint (when possible) to ensure compliance with access endpoint guidelines that may include running particular anti-virus or firewall software. Once it has been determined that the user is authorized to access the requested resource, a redirect can be issued that automatically sends the user on to their desired destination. The redirected request may include assertions, tokens, or other identifying data that can be used by the application for further validation, if desired.

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