To Pre-authenticate or Not to Pre-authenticate

Greg Coward, 2012-08-10

I'm bouncing around in the friendly skies, (turbulence sucks!) on my way back from the Microsoft Exchange conference and one question keeps rolling around in my head; how important is pre-authentication? Granted, it may not be a very compelling topic to most but with the recent announcement of TMG's end-of-life, it's at least relevant.

Along with other remote access / pre-authentication solutions, including F5's Access Policy Manager, (APM) many organizations from SMBs to large enterprises have utilized Microsoft's TMG, (Threat Management Gateway) to provide external pre-authentication for a variety of applications such as MS Exchange and SharePoint.

In a nutshell, reverse-proxy with pre-authentication, (aka remote access) solutions act as a secure doorway on the perimeter of the organization and prevent un-authenticated and un-trusted traffic from accessing resources residing on the private internal corporate network.

Now to be honest, there's not much debate in my mind around the value provided by pre-authentication at the edge of the Network. However, discontinuing the use of pre-authentication entirely in the light of TMG's demise was proposed as a possible solution. *Disclaimer --> This is not an official Microsoft recommendation but rather the opinion expressed by an individual presenter.* It's also important to mention that while TMG will no longer be offered as a product after December 1, 2012, mainstream support will still continue into 2015 which should give current users sufficient time to investigate and implement alternative solutions, (such as APM). Now with that said, I think it would behoove us all to quickly review some of what remote access solutions provide the organization before we tear the door off its hinges.

Isolation of Internal Domain-joined Resources

As I already mentioned pre-authentication resides at the perimeter of the organization's network and provides a layer of security further isolating internal resources from external access. Rather than allowing direct access to the internal resource, (an Exchange CAS server for example), only authenticated and authorized user connections will be able to pass into the corporate LAN. To provide a multi-layered perimeter security solution this functionality can be combined with other security systems such as IPS and layer 7 firewalls.

Multi-factor Authentication

I'll leave it up to you the reader to determine the value of multi-factor authentication. Regardless, whether it's username and password, certificates, hard/soft tokens, pre-defined security questions, adaptive auth, or any of the other various flavors of authentication methods available; many remote access solutions provide a much more secure authentication mechanism than what can be natively found on most applications. This is especially critical when we consider the vast and ever-growing number of devices organizations need to provide access for as a part of doing business.

Endpoint Inspection

To dovetail onto the previous comment, providing a username and password is simply not enough. In the age of BYOD, (**B**ring **Y**our **O**wn **D**evice), an organization should not only have confidence in who the user is that's accessing the corporate resource, (Exchange via ActiveSync for example) but have confidence that the device used to connect, (smartphone, corporate laptop, personal tablet, etc.) adheres to corporate policies. Some remote access solutions provide a means to identify and evaluate the client endpoint as part of the authentication/authorization process. For example, (*here comes a shameless plug*), utilizing APM on the F5 Big-IP with LTM can provide a means to manage access to corporate resources based upon the device trying to connect as well as ensuring the approved device adheres to corporate policies for such things as AV status, OS versions, patch levels, etc..

A Strategic Point of Control for Application Delivery

Pre-authentication / reverse-proxies provide a central point to administer access to multiple applications. Consider the alternatives. Without a reverse-proxy / pre-authentication solution access must be configured and controlled separately at each internal resource. All too often these internal resources, (such as Microsoft Exchange and SharePoint), are administered by different individuals or groups. What's more, independent access control makes applying corporate security policy consistently a challenge to say the least. On the contrary, implementing an application delivery controller like the F5 Big-IP with Access Policy Manager provides a strategic point of control where corporate applications can be deployed in a secure and consistent manner.

End-User Experience

It's not all about security. An application delivery controller that provides, among other things, pre-authentication can improve the user experience. Deploying applications behind the Big-IP with APM can provide single sign-on access as well as advanced application delivery. For example, once authenticated at the Big-IP users can access various corporate applications such as SharePoint and Exchange, often from a single namespace, while only needing to provide credentials once and often from a single namespace.

Latest F5 Information

- *F5 News Articles*
- *F5 Press Releases*
- *F5 Events*
- *F5 Web Media*
- *F5 Technology Alliance Partners*
- *F5 YouTube Feed*

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