F5 Tech Brief

Authentication 101

Authentication is a growing requirement in this new era of heightened technology security. What is authentication and how can it be implemented in your environment to meet all of your application needs?

by Kevin Stewart
Systems Engineer

Contents

What Is Authentication?

Authentication is the process of proving that you are who you say you are, usually for the purposes of gaining access to something. In the real world, this is a relatively easy task, even with a really bad driver's license photo; but in cyberspace, nothing is ever that simple. As a business owner, how do you know that the person accessing your ecommerce website is, in fact, the same person allowed to transfer funds on the site? From organized crime, to foreign governments, to pale-skinned teenagers in their parent's basement, there is great financial (and often personal) gain in defrauding businesses. The Internet provides a perfect haven for would-be thieves and mercenaries. It's big, distributed, uncensored, unmanaged, and very often anonymous. And your website, residing on the edge of that wild frontier, is a sitting duck. If you do any business online (or anywhere for that matter) that requires validation of the user's identity, then you need authentication. Authentication demands that the client prove that they are who they say they are, often in a variety of different ways: usernames and passwords, certificates, tickets, tokens, cookies, smart cards, biometrics, and so on. Authentication providers often use the word "factor" to classify each form of identity assertion. The more (different) factors used, the more secure the authentication. Also keep in mind that authentication is the "who you are" in access control, not the "what you can do." The latter is a concern of authorization, and authentication and authorization are not the same.

Authentication is complex. It's simply not good enough to check for the correct username and password in a database. In fact, many of the OWASP Top 10 web vulnerabilities relate to insecure authentication practices. Authentication methods are standardized but heavily interpreted. There are community standards for Kerberos, smart cards, biometrics, cookies, tokens, certificates, and many others, but every vendor implements them differently. If you've been in the IT business long enough, you've no doubt run across a few dozen different ways to authenticate to applications, and worse, have to remember a dozen or more complex passwords. As a result of the complexity required, authentication mechanisms tend to exert a big need for resources, resources that would otherwise be used by the applications requiring protection. Authentication is only as strong as its weakest link. It doesn't matter how cool your 4-factor biometric-token-smart card-password-based authentication solution is, if you're running it on Microsoft Windows 98 you might as well turn off the lights and go home.

So what's the answer to complex, semi-proprietary, resource heavy authentication mechanisms running on vulnerable software platforms? In a word: hardware. You need hardware-based SSL on a fast platform running a hardened OS, with the

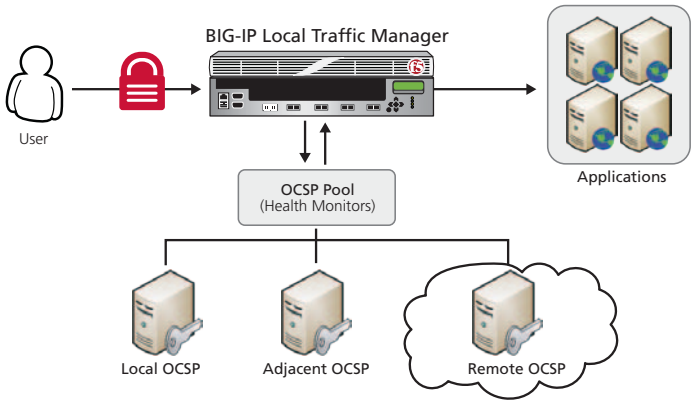
flexibility to do just about anything you want to do with authentication. The F5® BIG-IP® Local Traffic Manager™ (LTM) gives you just that. In the following sections, you'll get an idea of just some of the ways BIG-IP LTM can offload and improve on your complex authentication processes.

Certificate Revocation: Online Certificate Status Protocol

From basic server-side SSL (the "S" in HTTPS), to full-blown smart card deployments, Public Key Infrastructure (PKI) has become a cornerstone in authentication methodologies, especially in the government, financial, and medical sectors. PKI is based on a chain of trust from certificate issuer to certificate holder. In server-side PKI, the client must rely on the server by trusting its certificate and the issuer(s) of its certificate. In client-side PKI, the server trusts the client by validating the trust chain, and optionally the revocation status of that certificate. A certificate authority (CA) must publish a certificate revocation list (CRL) so that it can indicate revocation status of certificates it has issued. A CRL is a binary file—a list of revoked certificate serial numbers—and in some cases, depending on the level of activity of a particular CA, can get to be rather large. In order for a web server to validate the revocation status of a client certificate with a CRL, it must first download it, in whole. CRLs can be cached locally, but a potentially large binary file must still be parsed for each and every client certificate access request. Enter Online Certificate Status Protocol (OCSP). OCSP is a service that caches CRLs and responds to revocation status requests for single certificates. The server need only ask for the status of the current certificate. Not every application supports OCSP natively, however, so applications rely on third-party utilities installed locally to handle the requests. In any case, it's another layer of complexity that runs alongside your application, consuming valuable resources.

F5 BIG-IP LTM offloads OCSP, and the burden of software SSL encryption completely from the application server (in exchange for faster hardware SSL). By offloading this task, you can reclaim precious resources and know that BIG-IP LTM acts as an impenetrable fortress for all of your client certificate-based applications. Additionally, the typical configuration for an OCSP client, be it the application or third-party tool, is to simply list all of the OCSP services available to service status requests. If the selected OCSP server is incapable of servicing a request, the OCSP client must re-select another OCSP server and try again. With BIG-IP LTM you can create a pool of intelligently load balanced OCSP services and apply health monitors to ensure that your requests don't get sent to crippled servers. Consequently, if you

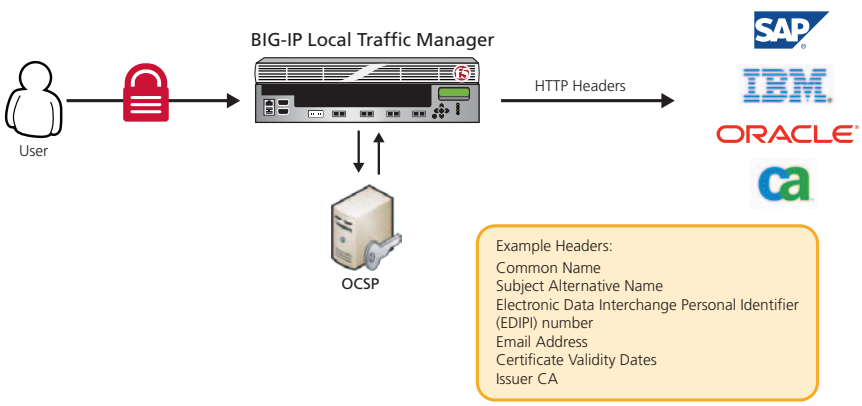
have your own OCSP services, or rely on other agencies, you can also prioritize the pool members so that the remote services aren't used unless the primary services are gone—a true high availability OCSP solution.



Load balancing, monitoring, and prioritizing OCSP services.

The Mighty HTTP Header

As simple as it seems, HTTP headers offer unparalleled power and flexibility for passing critical information to your application. Many commercial applications from vendors like Oracle, IBM, CA, and SAP can natively accept HTTP headers for authentication data. BIG-IP LTM provides this flexibility. So after passing that client certificate through an OCSP check, BIG-IP LTM can examine the full X.509 contents of the certificate, pull out, parse, re-order, and rebuild any pieces of data it needs and pass those as HTTP headers. In addition, because BIG-IP LTM is in complete control of this authentication data, a rogue client cannot inject their own HTTP headers to spoof the system.



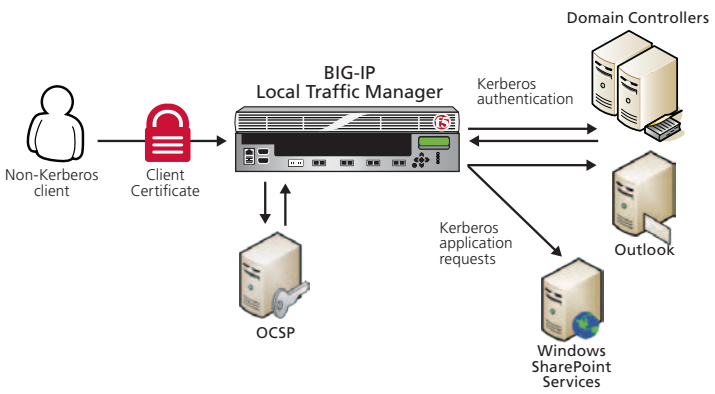
Inserting authentication data into HTTP headers.

Kerberos: The Microsoft Link

Kerberos is a complex protocol with a long, technical (and mythological) history. It's also the de facto authentication mechanism for many Microsoft products—like SharePoint and Outlook. In its simplest form, Kerberos creates a cryptographic system of mutual authentication—a system of "tickets," where each entity (client and server) grants ultimate authority to, and shares an encryption key with, a third-party: the Kerberos Key Distribution Center (KDC), commonly played by a Microsoft Active Directory domain controller. Originally designed to support username/password-based systems, Kerberos has also been extended to support public key cryptography. In fact, in order to authenticate to most Microsoft applications using PKI certificates, Kerberos must be involved. This is generally not a problem when the client and server are inside the domain and both able to communicate with, and get tickets from, the KDC/domain controller.

What about clients outside the domain? It's a pretty fair statement that most web applications are served primarily to clients outside the server's environment. Kerberos simply fails if the client cannot talk to the same domain controller(s). For that reason, Microsoft and others created Kerberos Protocol Transition (KPT). KPT enables non-Kerberos clients (clients unable to get Kerberos tickets from the server's domain controller) to pass through a service that "transitions" the client's authentication (whatever it may be) into a true Kerberos authentication request. The service effectively impersonates the client for all Kerberos transactions. It's a complicated interaction to say the least, and up until recently was only available with Microsoft Internet Security & Acceleration (ISA) server. While ISA has an impressive feature list, it is software running on a general purpose operating system (Microsoft Windows Server), which means it is highly dependent on the general purpose hardware platform on which it's installed and must be hardened, patched, and maintained frequently. Moreover, because ISA requires the entire client's certificate to enable KPT, it must also terminate the SSL stream. Terminating SSL anywhere else simply breaks client certificate password-less authentication.

If SSL cannot be terminated upstream by a load balancer, then load balancing persistence becomes increasingly unreliable (source IP address is the only available object to persist on, and that isn't reliable across public networks)—no persistence, no load balancing, unable to scale. BIG-IP LTM enables Kerberos Protocol Transition. With the combination of SSL offloading, certificate revocation checks, and header passing as well as the ability to transition a client's non-Kerberos requests into full domain Kerberos requests, BIG-IP LTM enables your architecture to scale infinitely and securely.



KPT Process:

1. Client requests access to SharePoint via BIG-IP LTM and presents certificate.
2. BIG-IP LTM validates certificate and generates an authentication service request **(AS_REQ)** to the domain on behalf of the client.
3. Domain returns a Ticket Granting Ticket **(TGT in AS_REP)** to BIG-IP LTM (acting as the client).
4. BIG-IP LTM generates a Ticket Granting Service request **(TGS_REQ)** to the domain for application access, passing the TGT.
5. Domain returns a service ticket for the requested application **(TGS_REP)**.
6. BIG-IP LTM generates an application request **(AP_REQ)** to the application, passing the service ticket.
7. Application returns its authenticator **(AP_REP)**, optionally, and the requested content.

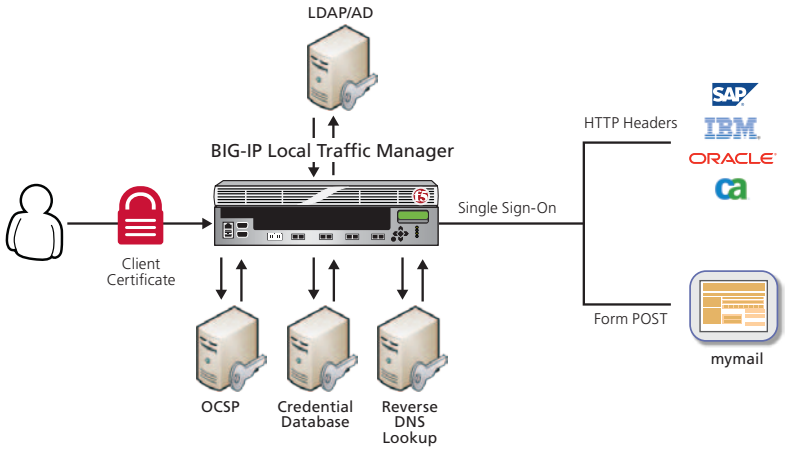
Kerberos protocol transition on BIG-IP LTM.

Ultimate Power and Flexibility with iRules

F5 iRules® scripting language is a patented F5 "network programming" environment. Based on industry standard Tool Control Language (TCL), iRules provide a simple, event-driven, scripting solution for all layer 4 to layer 7 data through BIG-IP LTM. This means you can programmatically read, write, and modify any data, for any protocol, in any direction. Want to redirect clients to HTTPS when they type HTTP in the browser? Or redirect clients to a different URL when they make specific requests? What if you need to inject, modify, or remove HTTP headers or cookies between the client and server? How about scrubbing social security and credit card numbers from outbound data to the client? All of these can be handled, easily, with iRules.

In addition, all of the authentication capabilities discussed thus far are accessible via iRules, and provide a virtual playground of possibilities. Take the results of an OCSP request, the contents of the client certificate, and perhaps an LDAP call, and push that data out as HTTP headers for both authentication ***and*** authorization information. Make application routing decisions based on the issuer or type of client certificate (smart card or software certificate). Access a database of credentials (or some identity management provider) and transparently post those credentials to a login form. Turn an application with weak, single-factor authentication into a secure multi-factor titan. Create an entire single sign-on environment across multiple applications, regardless of their individual implementations. Mix and match any of these ideas and others to create complex, rich, and secure authentication mechanisms for all of your applications.

Most of the authentication mechanisms are available right from the administration utility. Additional code assistance can be found on F5's developer community, DevCentral, which offers hundreds of working code samples and a user community of more than 60,000 IT professionals.



Authentication possibilities with BIG-IP LTM and iRules.

Other authentication capabilities in BIG-IP LTM include the ability to query an LDAP or Active Directory for username/password or certificate-base credentials. BIG-IP LTM also includes native support for RADIUS, TACACS+, and CRLDP (certificate revocation list distribution point) and KCD (Kerberos constrained delegation). KCD is similar to KPT except that the clients and servers are inside the domain. BIG-IP LTM acts a Kerberos proxy/forwarder when load balancing is required inside a network. In addition, with BIG-IP LTM, you can create a rich and secure single sign-on environment for all of your applications. Leveraging the flexibility of iRules and the built-in authentication capabilities of BIG-IP LTM, you can easily create a rich and secure enterprise client certificate single sign-on solution.

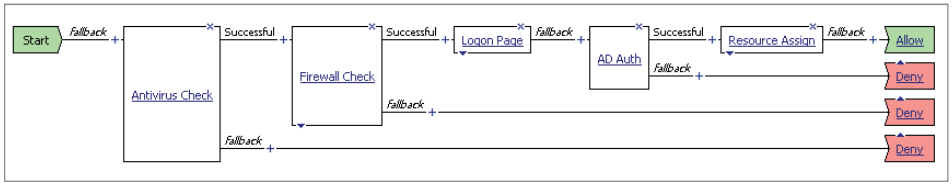
Secure Connections with BIG-IP Access Policy Manager

The F5 BIG-IP® Access Policy Manager™ (APM) provides users with secured connections to BIG-IP LTM virtual servers, specific web applications, or the entire corporate network. By leveraging standard web browsers and security technology, BIG-IP APM enables your corporation or organization to provide users access to various internal resources easily and cost-effectively, with no special software or configuration on the user's system. BIG-IP APM features and capabilities include:

- Standard browser support
- Enhanced privacy protection with RC4, Triple DES, and AES encryption
- Network access (an SSL VPN capability)
- Web application access (network access constrained to specific web applications)

- Client endpoint security (client firewall, antivirus, registry/file settings, and more)
- Full session auditing
- High availability and scalability
- A state-of-the-art visual policy editor
- Enhanced authentication capabilities

BIG-IP APM can perform authentication, authorization, and accounting (AAA), using standard AAA methods, including LDAP directories, Microsoft Active Directory and Windows domain servers, RADIUS servers, and HTTP authentication. BIG-IP APM also supports native RSA SecurID authentication, signed client digital certificates to authenticate devices, and native Oracle Access Manager (OAM) client/proxy functions.



The BIG-IP APM visual policy editor.

Conclusion

Your applications are critical to your business. Authentication and security are as important as performance and scalability. With BIG-IP LTM, you can offload and consolidate your authentication mechanisms and remove the complexity and heavy burden from already overloaded servers, improving application performance and security.

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.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

CS06-00011 0510