Offloading Remote Authentication for Servers

Overview

There are three phases most computers use to protect access to sensitive operations, applications, and data:

- *Identification* is the process the computer or application uses to identify the user. This usually consists of a user name.
- *Authentication* is the process by which a computer or application attempts to confirm the user is who they say they are using passwords, tokens, SSL certificates, etc.
- *Authorization* is when the application or computer decides what the user may do.

It's up to the corporation's IT staff to specify and enforce what that user is authorized to access. Most corporations authenticate users by asking for what they know, which is usually their password. With Internet access to most e-commerce and many business applications, many corporations could end up authenticating literally thousands of users.

Challenges

Managing authentication individually across your applications is costly. Top-level authentication enforcement consumes server cycles that could be used elsewhere. Configuring authentication for thousands of users is potentially error prone causing user frustration, lost productivity, lost revenue, or even unauthorized access. And, what happens when the authentication servers go down? For complete protection, authentication servers should be redundant and load balanced to guarantee authorized use.

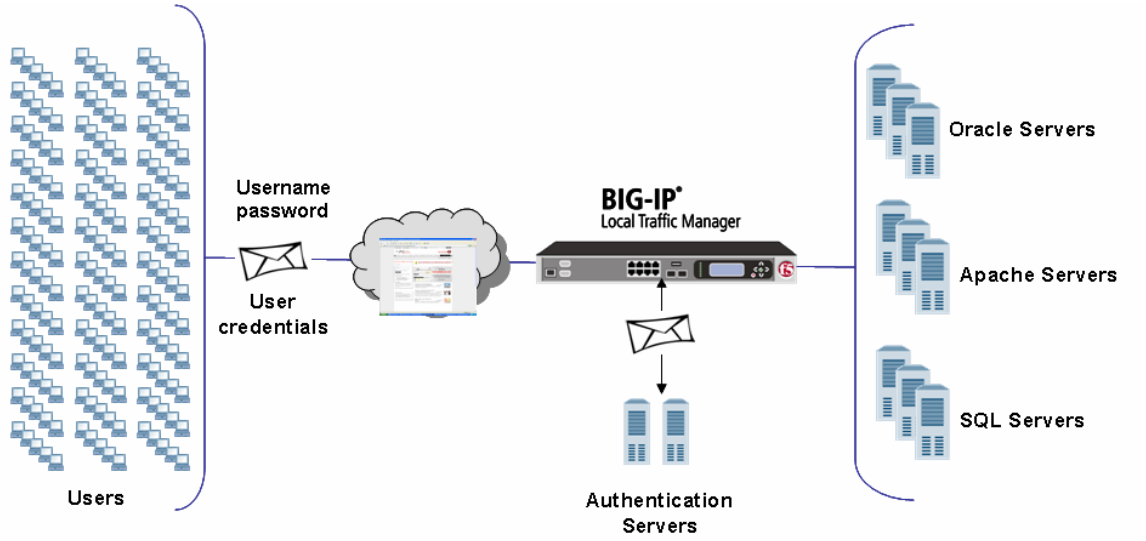
Solution

F5's Advanced Client Authentication

F5's Advanced Client Authentication software module for use with the BIG-IP® Local Traffic Manager provides client authentication of HTTP and other traffic types for a variety of authentication schemes, including LDAP, Radius, TACAS, SSL, and OCSP. The Advanced Client Authentication module with the BIG-IP Local Traffic Manager offers the following benefits:

- Provides a customizable authentication framework that gives you the ability to choose the authentication scheme that best fits your needs, and enables you to quickly change and deploy new authentication schemes as required.
- Reduces your TCO by centralizing application authentication to a single authentication cache, which reduces administrative burden, latency, and minimizes configuration errors.
- Increases server and application capacity by offloading authentication processing, including authentication of SSL certificates.
- Checks user credentials or SSL certificates using the authentication scheme of your choice before granting network access, stopping unwanted traffic before it reaches your servers and applications.
- Load balances authentication servers to continuously protect your network and application infrastructure.
- Reduces test and development efforts for web applications because all authentication is done at the BIG-IP device.

The following figure shows how the BIG-IP Local Traffic Manager increases your server capacity by offloading user authentication via remote authentication servers.



This paper describes how F5's Advanced Client Authentication module works to protect your application infrastructure while increasing your server capacity by offloading authentication processing.

Pluggable Authentication Module Technology

A significant feature of the BIG-IP Local Traffic Manager is its ability to support Pluggable Authentication Module (PAM) technology for passing client information to remote servers for authentication. This enables your application to leverage any number of PAMs to authenticate traffic.

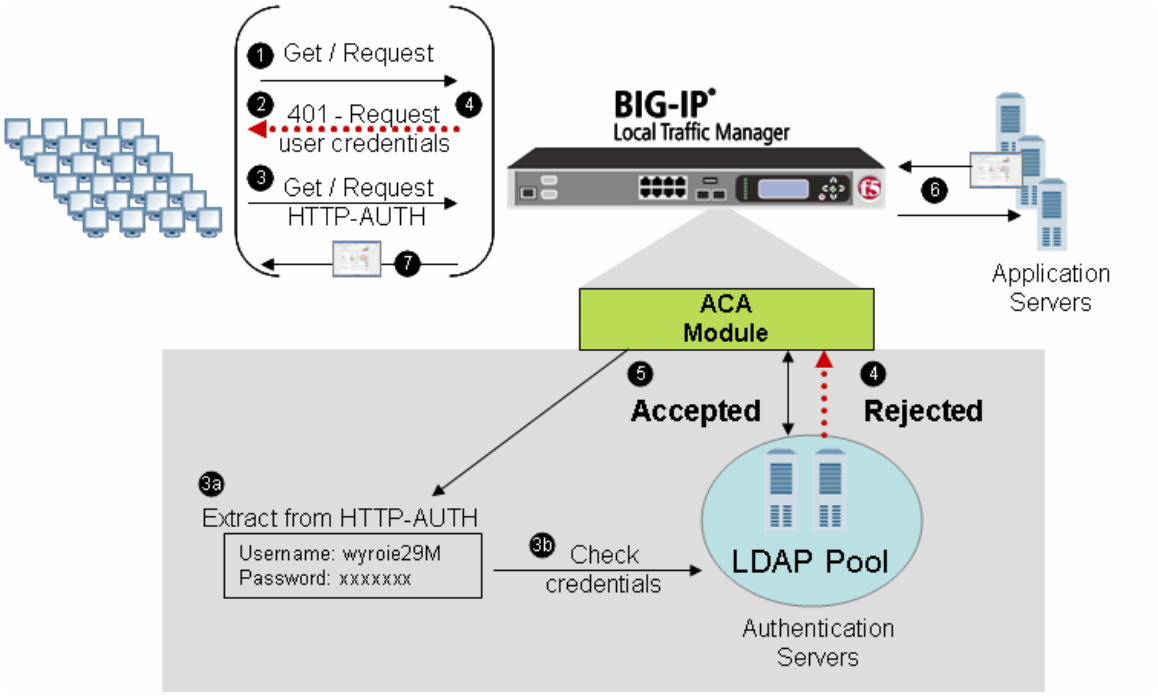
With the BIG-IP Local Traffic Manager acting as an authentication proxy for various types of traffic, enterprises can provide top-level authentication for applications at the BIG-IP device. This scheme pushes your security perimeter one level further away from your applications, offering a greater level of protection for your Web and application tiers.

By default, the BIG-IP system uses basic HTTP authentication (username, password) when remotely authenticating traffic. The procedure you use to set up remote authentication depends on the type of remote server you are using to store user accounts.

The following example shows the sequence of steps the BIG-IP uses to authenticate users.

1. The user sends a HTTP GET request to the server via BIG-IP.
2. The BIG-IP searches the user's HTTP request for an HTTP-AUTHENTICATE header, which contains the user's credentials. If it doesn't, the BIG-IP sends the user a 401 error message.
3. The user's browser prompts the user for credentials and sends the BIG-IP a new request with the user credentials encoded in the HTTP-AUTHENTICATE header.
    a. The BIG-IP extracts the credentials from the HTTP-AUTHENTICATE header.
    b. The BIG-IP forwards the credentials to the authentication server for authentication.
4. If the user credentials are missing or don't match the information that's stored in the authentication server, the BIG-IP sends the user a 401 message, requesting credentials.

5. If the user credentials match that information that's stored in the authentication server, the BIG-IP sends the user's request to the server to access the application.
6. The server retrieves the application that the user requested.
7. The BIG-IP forwards the application to the user.



Authentication Modules

The BIG-IP Local Traffic Manager supports different authentication schemes via authentication modules. These authentication modules enable you to use a remote system to authenticate application requests that pass through the BIG-IP Local Traffic Manager.

Using the BIG-IP Local Traffic Manager with the Advanced Client Authentication module, you can use any of the following kinds of authentication modules:

- **Lightweight Directory Access Protocol (LDAP)** authenticates network traffic using data stored on a remote LDAP server or a Microsoft® Windows Active Directory server. Client credentials are based on basic HTTP authentication (user name and password).
- **Remote Authentication Dial-In User Service (RADIUS)** authenticates network traffic using data stored on a remote RADIUS server. Client credentials are based on basic HTTP authentication (user name and password).
- **TACACS+** authenticates network traffic using data stored on a remote TACACS+ server. Client credentials are based on basic HTTP authentication (user name and password).
- **SSL client certificate LDAP** authorizes network traffic using data stored on a remote LDAP server. Client credentials are based on SSL certificates, as well as defined by user groups and roles.
- **Online Certificate Status Protocol (OCSP)** authenticates network traffic by checking the revocation status of a client certificate using data stored on a remote OCSP server. Client credentials are based on SSL certificates.

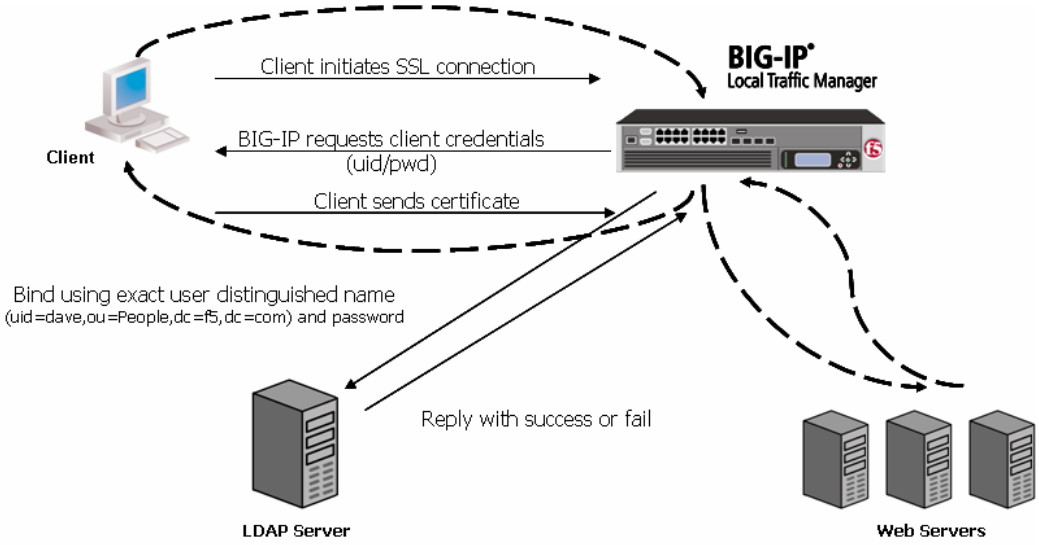
- **Universal Authentication** gives you the ability to identify and use variables passed in the HTTP header or payload for client authentication, including certificates or values that are communicated in the protocol. This is done using F5's iRules, a TCL-based programming language, and F5's Universal Inspection Engine to inspect, identify, and isolate traffic by the contents of their payload.

SSL Termination

If you are using SSL to protect your HTTP basic authentication traffic, you must configure the BIG-IP to perform the server-side SSL handshake that the remote server would normally do when authenticating traffic. This offloads SSL processing from your application servers, making your network more efficient.

LDAP Example

In the following example, the user wants to access a protected site (HTTPS). If the user responds with credentials, the BIG-IP constructs the user's distinguished name (using admin specified "base" and "key" values), and sends the user's distinguished name to the LDAP server along with their password. If the LDAP server verifies that the user's credentials are correct, the user is allowed access to the protected site. If the user's credentials are not correct, the BIG-IP severs the connection.



Advanced Capabilities

With the BIG-IP, you can employ advanced capabilities to:

- Apply filters to further specify what users can do
- Accept or reject user connections based on authentication results
- Authenticate users via virtual servers

The following sections describe each capability.

Filtering Roles and Groups

After locating the distinguished name in the LDAP database (essentially authentication), you can also use the BIG-IP to apply filters that further define what the user can do, for example:

- The user must possess a specific role
- The user must belong to a specific group

- Any other LDAP attributes may also be used as filters

The effect of filters is cumulative; if roles and groups are both specified, the user must possess both the role and belong to the group.

Accepting/Rejecting Failed Authorization Attempts

You can also configure the BIG-IP to reject or accept connections based on authorization results. This capability enables you to use F5 iRules to control traffic or enable servers to react differently to users who failed authentication (when customer configures mode to "accept"). For example, the BIG-IP can drop the connection when you configure the mode to "reject."

Remote Authentication to Virtual Servers

With the BIG-IP, you can authenticate users for virtual servers. This capability is implemented as a Profile using F5 iRules. The BIG-IP provides default Authentication iRules for LDAP, RADIUS, TACACS+, Client Cert LDAP and OCSP.

The following iRule returns a 401 error to the user in the event of a failure to authenticate the user's credentials.

```
when CLIENT_ACCEPTED {
        set tmm_auth_ldap_sid [AUTH::start pam default_ldap]
    }
    when HTTP_REQUEST {
        AUTH::username_credential $tmm_auth_ldap_sid [HTTP::username]
        AUTH::password_credential $tmm_auth_ldap_sid [HTTP::password]
        AUTH::authenticate $tmm_auth_ldap_sid
        HTTP::collect
    }
    when AUTH_SUCCESS {
        if {$tmm_auth_ldap_sid eq [AUTH::last_event_session_id]} {
            HTTP::release
        }
    }
    when AUTH_FAILURE {
        if {$tmm_auth_ldap_sid eq [AUTH::last_event_session_id]} {
            HTTP::respond 401
        }
    }
    when AUTH_WANTCREDENTIAL {
        if {$tmm_auth_ldap_sid eq [AUTH::last_event_session_id]} {
            HTTP::respond 401
        }
    }
    when AUTH_ERROR {
        if {$tmm_auth_ldap_sid eq [AUTH::last_event_session_id]} {
            HTTP::respond 401
        }
    }
```

Summary

F5's Advanced Client Authentication module with the BIG-IP Local Traffic Manager provides client authentication of HTTP and other traffic types for a variety of authentication schemes, including LDAP, Radius, TACAS, SSL, and OCSP. This authentication framework gives you the flexibility to use the authentication scheme that best fits your needs, and quickly change and deploy new authentication schemes as required. This design not only stops unwanted traffic before it reaches your servers and applications, but it also reduces your TCO by:

- Centralizing application authentication to a single authentication cache to reduce administrative burden, latency, and minimize configuration errors
- Increasing your server capacity by offloading authentication processing, including authentication of SSL certificates
- Reducing test and development efforts for web applications because all the authentication is done at the BIG-IP

Using the BIG-IP, you can also load balance your authentication servers to continuously protect your network and application infrastructure.

About F5 Networks

F5 Networks is the global leader in Application Delivery Networking. F5 provides solutions that make applications secure, fast, and available for everyone, helping organizations get the most out of their investment. By adding intelligence and manageability into the network to offload applications, F5 optimizes applications and allows them to work faster and consume fewer resources. F5's extensible architecture intelligently integrates application optimization, protection for the application and the network, and delivers application reliability – all on one universal platform. Over 10,000 organizations and service providers worldwide trust F5 to keep their applications running. The company is headquartered in Seattle, Washington with offices worldwide. For more information, go to www.f5.com.