

## 卸载服务器的远程认证 概述 挑战 解决方案

### 概述

大多数计算机利用三个阶段来访问敏感型操作、应用和数据：

- ☆ 身份确认是计算机或应用用来识别用户的阶段，通常利用用户名加以识别。
- ☆ 在认证阶段，计算机或应用试图进一步确认使用密码、令牌以及 SSL 认证的用户。
- ☆ 授权是应用或计算机确定用户在何时可以做什么。

企业的 IT 员工需要指定或控制经授权的用户所访问的内容。大多数企业认证用户被询问的通常是他们的密码。随着互联网访问大多数电子商务和多种业务应用，许多企业结束了这种认证数千用户的方式。

### 挑战

在应用中单独管理认证需要花费高昂的成本。高等级认证的执行消耗了可在其它地方发作用的服务器循环。为数千位用户配置认证可能会潜在地出现错误，导致用户无法正常工作、生产效率降低、收入减少甚或出现未授权的访问。当授权服务器停机时将发生什么情况？为了获得完善的保护，认证服务器应处于冗余状态且负载平衡，以保证经授权用户的顺利使用。

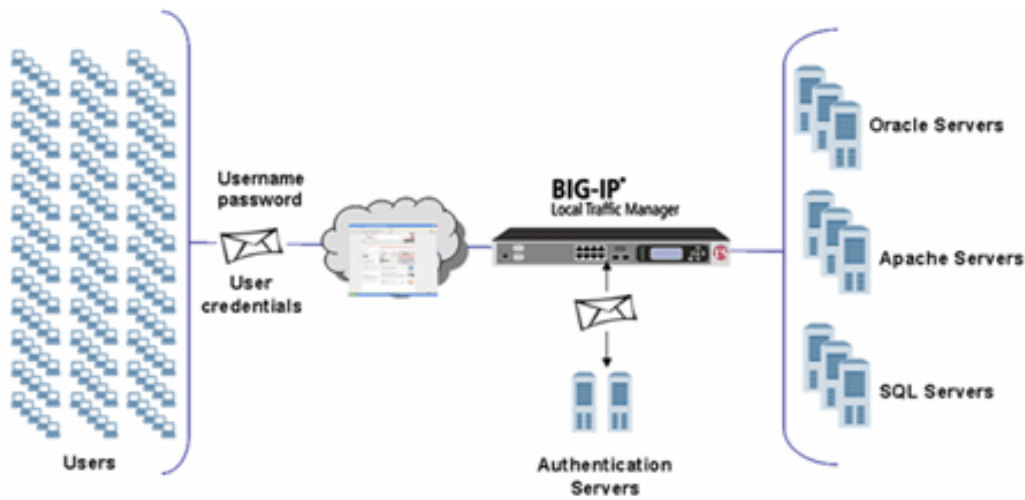
### 解决方案

#### F5 高级客户端认证

F5 高级客户端认证软件模块与 BIG-IP 本地流量管理器结合使用，为多种认证方案（包括 LDAP、Radius、TACAS、SSL 以及 OCSP）HTTP 及其它流量类型提供客户端认证。高级客户端认证模块与 BIG-IP 本地流量管理器结合使用可提供以下优势：

- ☆ 提供定制的认证架构，使您拥有选择最符合需求的认证方案的能力，并根据需求快速更改和部署全新的认证方案。
- ☆ 通过将应用认证集中至一个认证高速缓存可减轻管理负担、延迟并减少配置错误，从而缩减 TCO。
- ☆ 通过卸载认证流程（包括 SSL 证书的认证）来扩大服务器和应用容量。
- ☆ 利用您选择的认证方案在允许网络访问前检查用户的身份验证证书或 SSL 证书，在不合格的流量到达服务器和应用之前对其加以阻止。
- ☆ 实现认证服务器的负载平衡，以便为您的网络和应用基础设施提供连续的保护。
- ☆ 由于所有认证都是在 BIG-IP 设备上完成的，因此可减少 web 应用的测试和开发工作。

下图显示出 BIG-IP 本地流量管理器如何通过远程服务器采用卸载用户认证方式扩大服务器容量。



本文描述了 F5 高级客户端认证模块如何通过卸载认证流程来扩大服务器容量，从而保护您的应用基础设施。

### 可插拔认证模块技术

BIG-IP 本地流量管理器的主要特性是其支持可插拔认证模块 (PAM) 技术将客户端信息传递至远端服务器进行认证的能力。该特性支持您的应用充分利用任意数量的 PAM 来认证流量。

将 BIG-IP 本地流量管理器作为多种类型流量的认证代理，企业能够在 BIG-IP 设备上为应用提供高端认证。这种方案进一步巩固了应用的保护层，为您的 Web 和应用层提供了更高等级的保护。

缺省模式下，BIG-IP 系统利用基本的 HTTP 认证（用户名、密码）远程认证流量。您建立远程认证所采用的流程取决于您存储用户帐户所采用的远程服务器类型。以下实例显示出 BIG-IP 认证用户所采用的步骤顺序。

1. 用户通过 BIG-IP 向服务器发送 HTTP GET 请求。
2. BIG-IP 查找用户的 HTTP 请求用于 HTTP-AUTHENTICATE 报文头（包括用户的身份验证证书）。如果未经身份验证，则 BIG-IP 将向用户发送 401 错误信息。
3. 用户浏览器弹出以便用户进行验证并向 BIG-IP 发送带有用户身份验证证书（在 HTTP-AUTHENTICATE 报文头中编码）的新请求。
  1. BIG-IP 从 HTTP-AUTHENTICATE 报文头中提取用户身份验证证书。
  2. BIG-IP 将证书转发给认证服务器进行认证。
  0. 如果用户身份验证证书丢失或与存储于认证服务器中的信息不符，BIG-IP 则将向用户发送 401 错误信息，请求证书。
  0. 如果用户身份验证证书与存储于认证服务器中的信息匹配，BIG-IP 则将用户请求发送至服务器以便访问应用。
  0. 然后，服务器检索用户请求的应用。
  0. 最后，BIG-IP 将应用转发给用户。

### 认证模块

**BIG-IP** 本地流量管理器利用认证模块支持不同的认证方案。这些认证模块使您能够利用远程系统对通过 **BIG-IP** 本地流量管理器的应用请求进行认证。

利用具有高级客户端认证模块的 **BIG-IP** 本地流量管理器，您能够利用以下任意一种认证模块：

☆ 轻型目录访问协议 (**LDAP**) 利用存储于远程 **LDAP** 服务器或 **Microsoft Windows Active Directory** 服务器之上的数据对网络流量进行认证。客户端证书以基本的 **HTTP** 认证（用户名和密码）为依据。

☆ 远程认证拨号用户服务 (**RADIUS**) 利用存储于远程 **RADIUS** 服务器之上的数据对网络流量进行认证。客户端证书以基本的 **HTTP** 认证（用户名和密码）为依据。

☆ **TACACS+** 利用存储于远程 **TACACS+** 服务器之上的数据对网络流量进行认证。客户端证书以基本的 **HTTP** 认证（用户名和密码）为依据。

☆ **SSL** 客户端证书 **LDAP** 利用存储于远程 **LDAP** 服务器之上的数据对网络流量进行认证。客户端证书以 **SSL** 证书以及定义的用户群和角色为依据。

☆ 在线证书状态协议 (**OCSP**) 利用存储于远程 **OCSP** 服务器之上的数据，通过检查客户端证书的撤销状态对网络流量进行认证。客户端证书以 **SSL** 证书为依据。

☆ 通用认证支持您识别和利用 **HTTP** 报文头或负载中传递的变量用于客户端认证，包括在协议中通信的证书和值。利用 **F5** 的 **iRules**、基于 **TCL** 的编程语言以及 **F5** 的通用检查引擎进行检查、识别并根据其有效负载的内容分离流量。

## SSL 终端

如果您利用 **SSL** 保护 **HTTP** 基本的认证流量，那么，您必须对 **BIG-IP** 进行配置以执行服务器端 **SSL** 信息交换（通常当认证流量时远程服务器会进行如此操作）。从您的应用服务器中卸载 **SSL** 的流程可让您的网络具有更高效率。

## LDAP 举例

在下例中，用户希望访问一个受保护的站点 (**HTTPS**)。如果用户以身份验证证书作为响应，则 **BIG-IP** 创建用户标识名（利用管理员指定的“基本”和“密钥”值），并将用户标识名连同其密码发送至 **LDAP** 服务器。如果 **LDAP** 服务器验证出用户身份证书正确，则用户被允许访问受保护的站点。如果用户验证身份证书不正确，则 **BIG-IP** 将切断连接。

## 先进的性能

凭借 **BIG-IP**，您能够利用其先进的性能执行如下操作：

- ☆ 利用过滤器进一步明确用户能够执行的操作
- ☆ 接受或拒绝基于认证结果的用户访问
- ☆ 利用虚拟服务器对用户进行认证

以下章节介绍了每种性能。

## 过滤角色和用户群

将标识名放置于 LDAP 数据库（基本用于认证）中后，您还可利用 BIG-IP 采用过滤器进一步定义用户可执行的操作，例如：

- ☆ 用户必须具有特定的角色
- ☆ 用户必须属于一个特定的组
- ☆ 此外，其它 LDAP 属性也可能作为过滤器使用

过滤器的效果是累积的；如果角色和用户群都为特定属性，则用户必须拥有一个角色并属于一个用户组。

## 接受/拒绝失效的授权尝试

您还能够对 BIG-IP 进行配置，以拒绝或接受基于授权结果的连接。这种性能使您能够利用 F5 iRules 控制流量或支持服务器对于认证失败的用户发挥截然不同的作用（将模式配置为“接受”）。例如，将模式配置为“拒绝”时，BIG-IP 可切断连接。

## 虚拟服务器的远程认证

凭借 BIG-IP，您能够认证虚拟服务器的用户。利用 F5 iRules，这种性能与简档 (Profile) 相同。BIG-IP 为 LDAP、RADIUS、TACACS+、Client Cert LDAP 以及 OCSP 提供缺省的认证 iRules。

当认证用户身份认证证书发生故障时，以下 iRule 将向用户返回 401 错误信息。

```
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  
}  
}
```

## 总结

F5 高级客户端认证软件模块与 BIG-IP 本地流量管理器结合使用，为多种认证方案（包括 LDAP、Radius、TACAS、SSL 以及 OCSP） HTTP 及其它流量类型提供客户端认证。这种认证架构为您提供利用认证方案的出色的灵活性，从而最大限度的满足您的需求，并可根据需求快速更换和部署全新的认证方案。这种设计不仅能够不合格的流量到达服务器和应用之前对其加以阻止，还可通过以下方式降低您的总体拥有成本：

- ☆ 将应用认证集中至一个认证高速缓存来减轻管理负担、延迟并减少配置错误
- ☆ 通过卸载认证流程（包括 SSL 证书的认证）来扩大服务器和应用容量。
- ☆ 由于所有认证都是在 BIG-IP 设备上完成的，因此可减少 web 应用的测试和开发工作。
- ☆ 利用 BIG-IP，您还可以实现认证服务器的负载平衡，从而为您的网络和应用基础设施提供连续的保护。