

Transferindo a carga da autenticação remota dos servidores

Visão Geral Há três etapas usadas pela maioria dos computadores para proteger o acesso a operações, aplicativos e dados sensíveis:

- A identificação é o processo usado pelo computador ou aplicativo para identificar o usuário. Isso normalmente consiste em um nome de usuário.
- A autenticação é o processo pelo qual um computador ou aplicativo tenta confirmar que o usuário é quem afirma ser, usando senhas, tokens, certificados SSL, etc.
- A autorização é quando o aplicativo ou computador decide o que o usuário pode fazer.

É a equipe de TI da companhia que especifica e impõe o que o usuário está autorizado a acessar. A maioria das corporações autenticam os usuários solicitando uma informação, normalmente, a senha. Com o acesso pela Internet à maioria do comércio eletrônico e muitos aplicativos de negócios, muitas corporações podem, ao fim, autenticar literalmente milhares de usuários.

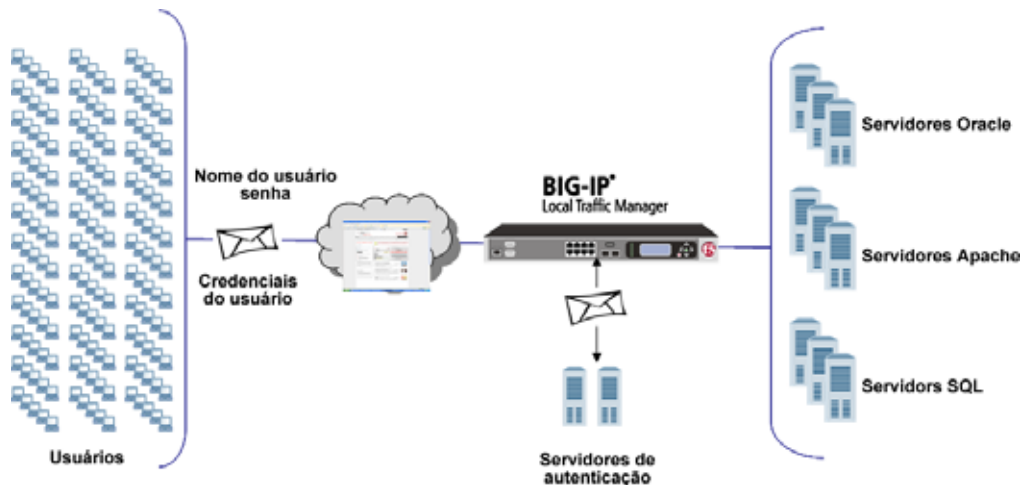
Desafios O gerenciamento individual da autenticação em todos os seus aplicativos é um processo caro. A imposição de autenticação de alto nível consome ciclos do servidor que poderiam ser utilizados em outra tarefa. Configurar a autenticação para milhares de usuários pode ocasionar erros, causando frustração aos usuários, perda de produtividade e receita e até mesmo acesso não autorizado. E o que acontece quando os servidores de autenticação ficam inativos? Para uma proteção completa, os servidores de autenticação devem ser redundantes e ter a carga balanceada para garantir o uso autorizado.

Solução Autenticação avançada de clientes da F5

O módulo de autenticação avançada de clientes da F5, para uso com o BIG-IP® Local Traffic Manager oferece a autenticação de clientes para tráfego HTTP e outros tipos, em vários esquemas de autenticação, incluindo: LDAP, Radius, TACAS, SSL e OCSP. O módulo de autenticação avançada de clientes, em conjunto com o BIG-IP Local Traffic Manager, oferece os seguintes benefícios:

- Fornece uma estrutura de trabalho personalizada de autenticação que dá a você a capacidade de escolher o esquema de autenticação mais adequado às suas necessidades e lhe permite mudar ou implementar novos esquemas de autenticação rapidamente, conforme a necessidade.
- Reduz o custo total de propriedade centralizando a autenticação de aplicativos em um único cache de autenticação, diminuindo a carga administrativa, a latência e minimizando erros de configuração.
- Aumenta a capacidade de servidores e aplicativos transferindo a carga do processamento de autenticação, incluindo a autenticação de certificados SSL.
- Verifica as credenciais do usuário ou certificados SSL usando o esquema de autenticação de sua escolha antes de conceder acesso à rede, detendo o tráfego indesejado antes que ele atinja seus servidores e aplicativos.
- Faz o balanceamento de carga dos servidores de autenticação para proteger continuamente a sua infra-estrutura de rede e aplicativos.
- Reduz os esforços de teste e desenvolvimento para aplicativos web, pois toda a autenticação é feita no dispositivo BIG-IP.

A imagem abaixo mostra como o BIG-IP LTM aumenta a capacidade do seu servidor transferindo a carga da autenticação do usuário por meio de servidores remotos de autenticação.



Este documento descreve como o módulo de autenticação avançada de clientes da F5 trabalha para proteger a sua infra-estrutura de aplicativos enquanto incrementa a capacidade do seu servidor transferindo a carga do processamento de autenticação.

Tecnologia do módulo plugável de autenticação

Uma função importante do BIG-IP LTM é a capacidade de suportar a tecnologia do módulo plugável de autenticação (PAM) para passar informações dos clientes aos servidores remotos para fins de autenticação. Isso permite que o seu aplicativo use qualquer número de PAMs para autenticação de tráfego.

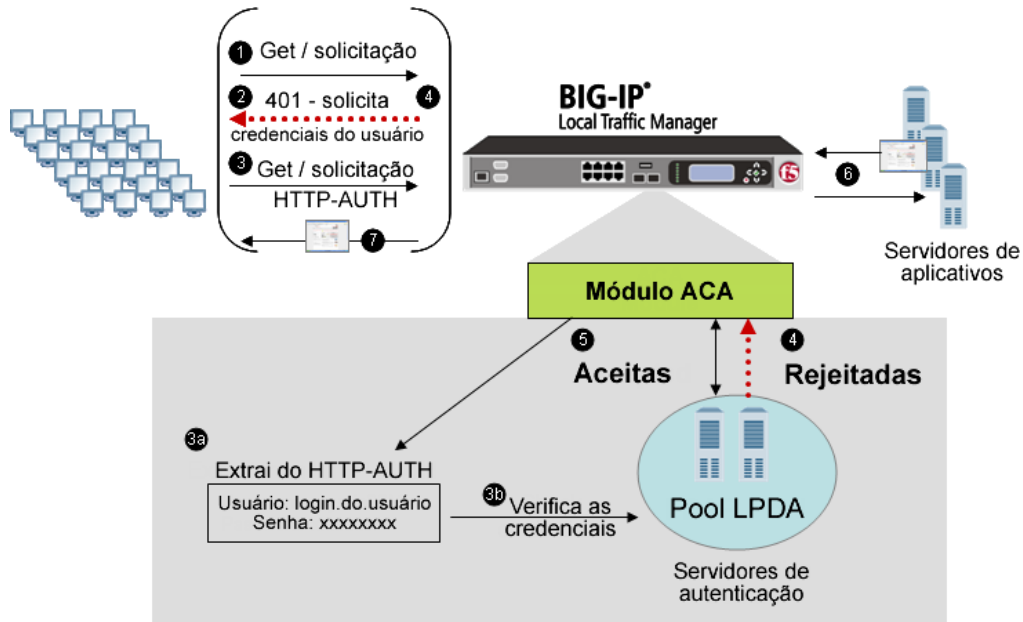
Com o BIG-IP Local Traffic Manager agindo como proxy de autenticação para vários tipos de tráfego, as companhias podem fornecer autenticação de alto nível no dispositivo BIG-IP. Esse esquema coloca o seu perímetro de segurança em um nível acima dos aplicativos, oferecendo um alto grau de proteção para as camadas web e de aplicativos.

Por padrão, o BIG-IP usa autenticação HTTP básica (nome de usuário, senha) na autenticação remota do tráfego. O procedimento usado para configurar a autenticação remota depende do tipo de servidor remoto que você usa para armazenar as contas de usuário.

O exemplo a seguir mostra a seqüência de passos usada pelo BIG-IP para autenticar usuários.

1. O usuário envia uma solicitação HTTP GET ao servidor via BIG-IP.
2. O BIG-IP verifica a solicitação HTTP do usuário e localiza o cabeçalho HTTP-AUTHENTICATE, que contém as credenciais do usuário. Se as credenciais não estiverem presentes, o BIG-IP envia uma mensagem de erro 401 para o usuário.
3. O navegador do usuário solicita as credenciais e envia uma nova solicitação ao BIG-IP, com as credenciais do usuário codificadas no cabeçalho HTTP-AUTHENTICATE.
 - a. O BIG-IP extrai as credenciais do cabeçalho HTTP-AUTHENTICATE.
 - b. O BIG-IP encaminha as credenciais para o servidor de autenticação.
4. Se as credenciais do usuário não estiverem presentes ou não combinarem com as informações armazenadas no servidor de autenticação, o BIG-IP envia uma mensagem 401 ao usuário, solicitando as credenciais.

5. Se as credenciais do usuário combinarem com as informações armazenadas no servidor de autenticação, o BIG-IP envia o pedido do usuário ao servidor, para acessar o aplicativo.
6. O servidor recupera o aplicativo solicitado pelo usuário.
7. O BIG-IP encaminha o aplicativo ao usuário.



Módulos de autenticação

O BIG-IP Local Traffic Manager suporta diferentes esquemas de autenticação, por meio de módulos de autenticação. Esses módulos de autenticação e permitem que você use um sistema remoto para autenticar solicitações de aplicativos que passam pelo BIG-IP LTM.

Usando o BIG-IP Local Traffic Manager com o módulo de autenticação avançada de clientes, você pode usar qualquer um dos seguintes tipos de módulos de autenticação:

- Lightweight Directory Access Protocol (LDAP) autentica o tráfego de rede usando dados armazenados em um servidor LDAP remoto ou um servidor com o Microsoft® Windows Active Directory. As credenciais dos clientes são baseadas na autenticação HTTP básica (nome de usuário e senha).
- Remote Authentication Dial-In User Service (RADIUS) autentica o tráfego de rede usando dados armazenados em um servidor RADIUS remoto. As credenciais dos clientes são baseadas na autenticação HTTP básica (nome de usuário e senha).
- TACACS+ autentica o tráfego de rede usando dados armazenados em um servidor TACACS+ remoto. As credenciais dos clientes são baseadas na autenticação HTTP básica (nome de usuário e senha).
- O certificado de cliente SSL do LDAP autoriza o tráfego de rede usando dados armazenados em um servidor LDAP remoto. As credenciais do cliente são baseadas em certificados SSL e também definidas em grupos de usuários e funções.
- Online Certificate Status Protocol (OCSP) autentica o tráfego de rede verificando o estado de revogação do certificado de um cliente usando dados armazenados

em um servidor OCSP remoto. As credenciais dos clientes são baseadas em certificados SSL.

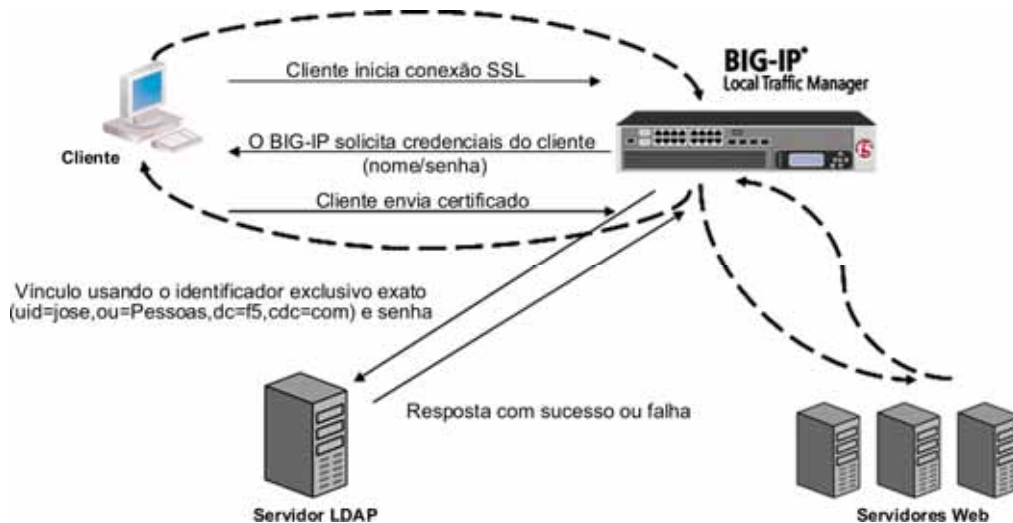
- A autenticação universal dá a você a capacidade de identificar e usar variáveis passadas pelo cabeçalho ou conteúdo da solicitação HTTP para a autenticação de clientes, incluindo certificados ou valores comunicados no protocolo. Isso é feito usando as iRules da F5, uma linguagem de programação baseada em TCL, e a Universal Inspection Engine da F5, para inspecionar, identificar e isolar tráfego pelo conteúdo.

Encerramento SSL

Se você está usando SSL para proteger seu tráfego de autenticação HTTP básica, deve configurar o BIG-IP para executar o handshake normalmente feito pelo servidor remoto ao autenticar tráfego. Isso transfere a carga do processamento SSL dos seus servidores de aplicativos, tornando sua rede mais eficiente.

Exemplo LDAP

No exemplo abaixo, o usuário quer acessar um site protegido (HTTPS). Se o usuário responder com credenciais, o BIG-IP cria um identificador distinto para o usuário (usando valores "base" e "chave" determinados pelo administrador) e o envia, com a senha, ao servidor LDAP. Se o servidor verificar que as credenciais do usuário estão corretas, o usuário poderá acessar o site protegido. Se as credenciais não estiverem corretas, o BIG-IP encerra a conexão.



Capacidades avançadas

Com o BIG-IP, você pode utilizar capacidades avançadas para:

- Aplicar filtros para especificar ainda mais o que os usuários podem fazer
- Aceitar ou rejeitar conexões de usuários com base nos resultados da autenticação
- Autenticar usuários por meio de servidores virtuais

As seções a seguir descrevem cada capacidade.

Filtrando grupos e funções

Após localizar o identificador na base de dados LDAP (basicamente, autenticação), você também pode usar o BIG-IP para aplicar filtros que define especificamente o que o usuário pode fazer, por exemplo:

- O usuário deve possuir uma função específica

- O usuário deve pertencer a um grupo específico
- Qualquer outro atributo LDAP pode ser usado como filtro

O efeito dos filtros é cumulativo; se forem especificados funções e grupos, o usuário deverá possuir a função e pertencer ao grupo.

Aceitando/rejeitando tentativas malsucedidas de autenticação

Você também pode configurar o BIG-IP para rejeitar ou aceitar conexões com base nos resultados da autorização. Essa capacidade lhe permite usar as iRules da F5 para controlar o tráfego ou permitir que servidores reajam de forma diferente aos usuários com autenticação malsucedida (quando o cliente configura o modo para "aceitar"). Por exemplo, o BIG-IP pode encerrar a conexão se você configurar o modo para "rejeitar".

Autenticação remota para servidores virtuais

Com o BIG-IP, você pode autenticar usuários para servidores virtuais. Essa capacidade é implementada como um perfil, usando as iRules da F5. O BIG-IP fornece iRules padronizadas de autenticação para LDAP, RADIUS, TACACS+, certificados de cliente LDAP e OCSP.

A iRule a seguir envia um erro 401 ao usuário em caso de falha da autenticação das credenciais.

```
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
  }
}
```

Resumo

O módulo de autenticação avançada de clientes da F5, para uso com o BIG-IP® Local Traffic Manager, oferece a autenticação de clientes para tráfego HTTP e outros tipos, em vários esquemas de autenticação, incluindo: LDAP, Radius, TACAS, SSL e OCSP. Essa estrutura de trabalho de autenticação lhe dá a flexibilidade de usar o esquema de autenticação mais indicado às suas necessidades e de mudar e implementar rapidamente novos esquemas de autenticação conforme o necessário.



Esse design não apenas detém o tráfego indesejado antes que alcance seus servidores e aplicativos como também reduz seu custo total de propriedade:

- Centralizando a autenticação de aplicativos em um único cache de autenticação para reduzir a carga administrativa, a latência e minimizar os erros de configuração
- Aumentando a capacidade dos servidores, transferindo a carga do processamento de autenticação, incluindo a autenticação de certificados SSL
- Reduzindo os esforços de teste e desenvolvimento para aplicativos web, pois toda a autenticação é feita no dispositivo BIG-IP

Usando o BIG-IP, você também pode balancear a carga dos seus servidores de autenticação para proteger continuamente sua infra-estrutura de rede e aplicativos.

Sobre a F5

A F5 Networks é a líder global em Application Delivery Networks. A F5 fornece soluções que tornam os aplicativos seguros, rápidos e disponíveis para todos, ajudando as companhias a obter o maior retorno pelo seu investimento. Ao implementar inteligência e gerenciabilidade na rede para transferir a carga de aplicativos, a F5 os otimiza, permitindo que eles trabalhem mais rápido e consumam menos recursos. A arquitetura expansível da F5 integra de forma inteligente a otimização de aplicativos, protege os aplicativos e a rede e oferece confiabilidade aos aplicativos - tudo em uma plataforma universal. Mais de 10.000 companhias e provedores de serviços em todo o mundo confiam na F5 para manter seus aplicativos funcionando. A companhia tem sede em Seattle, Washington, com escritórios no mundo todo. Para mais informações, visite www.f5.com (em inglês).