



Documento da F5

# Segurança Gerenciável de Aplicativos

O BIG-IP Application Security Manager v10.1 fornece a visibilidade, o controle e a flexibilidade necessários para defender as aplicações e cumprir as leis sem sacrificar a capacidade gerencial.

por **Lori MacVittie**

Gerente Técnico de Marketing, Serviços de Aplicação



# Índice

<b>Resumo Executivo ou Introdução</b>	<b>3</b>
<hr/>	
<b>Visibilidade</b>	<b>3</b>
Relatórios	4
Raspagem na Web	5
Sistema Especialista em Ataques	5
<hr/>	
<b>Controle</b>	<b>6</b>
Preparação	7
iRules	7
<hr/>	
<b>Flexibilidade</b>	<b>8</b>
Possibilitando as Auditorias Externas	8
Opções de Integração	9
<hr/>	
<b>Conclusão</b>	<b>11</b>



## Introdução

Gerenciável é um termo raramente usado com segurança de aplicação na mesma frase, particularmente com segurança de aplicação web. As metodologias de implementação agressivas e ágeis combinadas com a descoberta de novos (e variação de antigos) vetores de ataque, põem constante pressão sobre a equipe de segurança da informação e sobre as soluções que ela emprega para defender as aplicações web.

Parte do problema é a quantidade de informação que precisa ser coletada, conferida, esmiuçada e resumida para os diretores e acionistas da empresa, além dos desenvolvedores de aplicação web. A equipe de segurança da informação enfrenta uma sobrecarga de informação quase diariamente, e precisa peneirar um sem-número de artigos, relatórios, blogs, registros e verificações para conseguir fazer seu trabalho. Informação é vital para o sucesso das estratégias de segurança da aplicação web, como informações sobre um novo ataque, uma reviravolta em um ataque existente ou a identificação de pontos fracos nas aplicações web. Os investimentos em soluções de segurança precisam provar seu valor com clareza, o que leva a gastar tempo coletando e documentando as provas desse valor.

A última versão do F5® BIG-IP® Application Security Manager™ (ASM), v10.1, enfrenta essa sobrecarga de informação e a necessidade de agilidade na implementação. O lançamento do BIG-IP ASM inclui uma variedade de novos avanços tecnológicos na segurança da aplicação web que ajudam na sua defesa; novas opções de relatório e configuração para tornar a coleta e a agregação dos dados de segurança acessíveis com mais simplicidade; e uma melhor integração com as soluções da F5 e de parceiros planejada para aprimorar o tempo total de implementação, bem como a profundidade e a amplitude da informação disponível.

## Visibilidade

Para que as estratégias de segurança de aplicação web tenham sucesso, os administradores precisam ver os ataques, as políticas e a postura das aplicações frente às ameaças. Compreender qual é e como funciona o ataque, bem como as técnicas de atenuação usadas pelos firewalls de aplicação web, tem valor inestimável tanto por possibilitar a proteção quanto por instruir os administradores e desenvolvedores sobre o ataque.

O BIG-IP ASM v10.1 aborda as três áreas de visibilidade com recursos novos e aprimorados que fornecem a informação necessária para se atingir os objetivos de segurança.



## Relatórios

Relatórios são um fato inescapável no mundo da TI. No reino da segurança da aplicação web, eles são ainda mais importantes porque geralmente contêm as informações vitais para manter ágeis as estratégias de segurança da aplicação web e garantir a conformidade com as leis e normas, como as do PCI.

No passado, quando os administradores precisavam de relatórios sobre os ataques, violações, pistas de auditoria e vulnerabilidades, eles empregavam um servidor syslog centralizado. A menos que as organizações tenham sistemas externos para lidar com o agendamento ou a compilação de relatórios específicos para a segurança, esse processo pode ser penoso e consumir uma enormidade de tempo.

O BIG-IP ASM v10.1 apresenta um sistema de relatórios totalmente novo que permite tanto o agendamento quanto a personalização. Essa nova versão combina um servidor syslog externo para relatórios sobre tendências e coleta de dados forenses com uma variedade de opções de relatórios. As opções detalhadas na nova GUI permitem que os administradores explorem e encontrem com facilidade a informação de que precisam, quando precisam, sem ter de consultar sistemas externos. Além disso, o BIG-IP ASM v10.1 inclui 17 relatórios pré-configurados que dão visibilidade sobre os ataques e os padrões de uso.

#	Requirement	Compliance State	Details
1	Install and maintain a firewall configuration to protect cardholder data	N/A	N/A
2	Do not use vendor-supplied defaults for system passwords and other security parameters	✓	<a href="#">View Details</a>
3	Protect stored cardholder data	✓	<a href="#">View Details</a>
4	Encrypt transmission of cardholder data across open, public networks	✓	<a href="#">View Details</a>
5	Use and regularly update anti-virus software	N/A	N/A
6	Develop and maintain secure systems and applications	✓	<a href="#">View Details</a>
7	Restrict access to cardholder data by business need-to-know	N/A	N/A
8	Assign a unique ID to each person with computer access	✓	<a href="#">View Details</a>
9	Restrict physical access to cardholder data	N/A	N/A
10	Track and monitor all access to network resources and cardholder data	✓	<a href="#">View Details</a>
11	Regularly test security systems and processes	N/A	N/A
12	Maintain a policy that addresses information security	N/A	N/A

Figura 1: Um novo relatório de conformidade com PCI no BIG-IP ASM v10.1 ajuda as organizações a compreender a conformidade.



O novo sistema de relatório inclui dados de geolocalização altamente precisos. Os relatórios com localização fornecem informações sobre o país de origem das ameaças. A isso se juntam a nova capacidade de configurar o BIG-IP ASM para usar o cabeçalho HTTP XFF (X transfere para) nos relatórios e os cálculos usados para detectar os ataques de força bruta e DoS na L7. Essas capacidades ajudam os clientes que usam serviços como Akamai, no qual algumas das requisições passaram por proxies. A capacidade de configurar o BIG-IP ASM estreita a identificação dos infratores e, em conjunto com a geolocalização, pode ser uma ferramenta inestimável para reforçar as políticas de prevenção de ataques distribuídos.

## Raspagem na Web

A raspagem na web, ou web scraping, é uma técnica antiga ainda usada por algumas razões. Embora tenha sido empregada originalmente para transportar as aplicações de tela verde ou antigas para a web e fornecer métodos de integração para outras aplicações inacessíveis, hoje é usada para coletar endereços de e-mail, dados sigilosos e para encontrar as vulnerabilidades que poderiam ser exploradas. A atividade de bot geralmente é usada para melhorar a classificação de determinados termos de pesquisa ao automatizar o processo de geração de novas páginas das plataformas web. Outro uso ilegítimo das técnicas de raspagem na web é conhecido com "web spam".

A raspagem na web, hoje, não é considerando um problema clássico de segurança, e sim está mais relacionada a roubo de dados. Se um concorrente seu coleta seus dados e os publica, isso pode distorcer sua marca ou mudar a forma de apresentação do conteúdo, afetando negativamente o impacto dos dados nos seus objetivos comerciais. Os métodos tradicionais de identificar bots e aranhas (que são automatizados) não detectam com precisão as atividades de raspagem pelas similaridades entre os usuários humanos e os dados automatizados.

Além de aumentar a visibilidade e a proteção, a nova tecnologia de detecção da raspagem web do BIG-IP ASM fornece informações valiosas sobre esses tipos de ataque. Seja aranhas ou navegadores usando scripts, o BIG-IP ASM fornece os meios necessários para a detecção de tais ataques. Embora não seja infalível, o BIG-IP ASM analisa o comportamento e as características da navegação para determinar se um ataque está em andamento e pode impedi-lo ou apenas reportar a violação.

## Sistema Especialista em Ataques

Conforme as ameaças se tornam mais numerosas e complexas, torna-se cada vez mais difícil para os administradores e para as equipes de segurança da informação se manterem a par de cada ataque e contramedida. O BIG-IP ASM v10.1 apresenta um novo e amplo sistema especialista em ataques que fornece a descrição imediata e detalhada do ataque, além de melhorar a visibilidade das técnicas de atenuação usadas pelo BIG-IP ASM para detectar e evitar o ataque. O sistema especialista também ajuda as equipes de rede (que geralmente são responsáveis pelo gerenciamento dos firewalls de aplicação web e dispositivos similares) a se familiarizar com a segurança da aplicação web.



Cada violação detectada pelo BIG-IP ASM também inclui o risco associado com a violação/verificação e um exemplo de ataque. Apresentar ambos, o risco e um exemplo, junto com as informações de violação ajuda os administradores e desenvolvedores a empregar uma solução baseada no risco e na dificuldade de implementação.



Figura 2: Novo sistema especialista em ataque fornece informações detalhadas sobre ataques, riscos e técnicas de atenuação.

## Controle

Um dos aspectos mais difíceis no gerenciamento de um firewall de aplicação web é lidar com as mudanças quase ininterruptas das políticas, decorrentes das frequentes modificações no site. Quando as políticas são ajustadas automaticamente para as alterações da aplicação, elas precisam ser reverificadas para garantir a precisão. Esse processo é tão difícil quanto determinar o melhor meio de restringir o acesso aos clientes. Ambas as tarefas requerem um equilíbrio delicado para garantir o controle de segurança mais rígido possível sem comprometer o acesso do usuário legítimo. Isso implica que as alterações sugeridas precisam ser examinadas e testadas para garantir que os infratores sejam punidos com a maior precisão possível sem impactar os usuários legítimos.

O BIG-IP ASM v10.1 inclui tipos adicionais de objeto nas políticas de preparação, integração com o F5 iRules™ para melhorar a personalização e a flexibilidade e penalidades por IP para infratores recorrentes.



## Preparação

A preparação de políticas não é um conceito novo na segurança da aplicação web nem no BIG-IP ASM. Entretanto, o BIG-IP ASM v10.1 inclui tipos de arquivo, URLs e parâmetros. As políticas podem conter objetos que se alteram frequentemente em uma aplicação web. As políticas apenas para objetos podem ser preparadas para testes transparentes em ambientes de produção, deixando todas as outras entidades de política em modo de bloqueio. A preparação permite testar e atualizar as políticas até que estejam preparadas para serem promovidas a políticas de segurança de aplicação prontas, capazes de bloquear corretamente sem reduzir os níveis atuais de proteção.

## iRules

O BIG-IP ASM v10.1 agora se integra ao iRules, a plataforma da F5 de implementação de scripts. Os novos eventos do iRules específicos para as violações do BIG-IP ASM dão mais flexibilidade para os administradores responderem aos dados e ataques maliciosos. Por exemplo, uma página personalizada de resposta pode ser retornada baseada na violação específica, fornecendo mais informações sobre o ataque. Os dados fornecidos por usuários suspeitos podem ser manipulados para atenuar o ataque, o que é útil se os dados foram alterados ou corrompidos sem o consentimento do usuário, ou os administradores podem preferir forçar o logout do usuário pela violação.

As respostas aos ataques variam entre as organizações e pelo tipo de violação, portanto, é inviável pré-definir na solução todas as possíveis repostas de segurança da aplicação web. Por isso, a integração com o iRules foi incluída no BIG-IP ASM v10.1 para permitir controlar o comportamento da política de segurança da aplicação web e suprir melhor as necessidades da organização de TI e da empresa.

## Penalidades de IP

Com o BIG-IP ASM v10.1 é possível restringir o acesso de um IP único que gerar muitas violações por um período de tempo. Esse controle granular da violação permite restringir ou bloquear completamente o acesso dos endereços IP com histórico de violação de políticas, o qual indicaria um possível ataque em andamento.

Combinado com o uso da geolocalização e o cabeçalho XFF, esse novo recurso permite que os administradores controlem com precisão as requisições dos clientes e evitem uma sobrecarga das aplicações e da infraestrutura interna com as tentativas repetidas de acesso não autorizado.



## Flexibilidade

Flexibilidade é fundamental na segurança da aplicação web por causa das alterações frequentes no ambiente e nos métodos de ataque. Uma solução para a segurança de aplicação web estática, inflexível, pode fornecer uma proteção excelente para as aplicações web em um determinado momento, porém não fornece às organizações a capacidade de se adaptar aos novos ataques, conteúdos ou requisições de usuário.

A capacidade de se integrar com soluções de terceiros que fornecem serviços complementares é de extrema importância. A integração com o restante da infraestrutura é a marca de uma infraestrutura dinâmica, e gera uma solução de segurança mais dinâmica e adaptativa. O BIG-IP ASM v10.1 permite esse tipo de integração e, nesse lançamento, aprimora a sua integração com o Sentinel da WhiteHat Security para melhorar a integração em geral.

A integração não está limitada apenas às soluções de terceiros. Quando uma solução de segurança da aplicação web como o BIG-IP ASM é empregada em uma plataforma de serviços unificados de dados e fornecimento de aplicação, como o BIG-IP® Local Traffic Manager™ (LTM), espera-se que ela se integre bem às outras soluções na mesma plataforma. O BIG-IP ASM v10.1 se integra perfeitamente aos recursos e aos módulos adicionais do BIG-IP LTM, apoiando uma infraestrutura unificada e de alto desempenho no fornecimento de aplicação.

Os profissionais e os administradores da segurança de aplicação web precisam poder examinar e auditar a postura de segurança de toda a infraestrutura, incluindo as políticas de segurança da aplicação web. Como essas políticas também se integram aos esforços de conformidade, é importante que o firewall de aplicação web possa fornecer informações detalhadas e compreensíveis para aqueles que não estão familiarizados com o sistema. Para atingir esses objetivos, o BIG-IP ASM v10.1 exporta as políticas para um formato que possa ser lido por humanos.

## Possibilitando as Auditorias Externas

As políticas do BIG-IP ASM podem ser exportadas para um arquivo XML legível. Qualquer um pode ler e compreender as políticas que governam a segurança web sem precisar acessar fisicamente o console ou a GUI e sem precisar de um treinamento intenso para interpretar as opções de configuração.

Isso é particularmente útil durante os processos de auditoria do PCI com um auditor externo ou quando não se tem acesso ao BIG-IP ASM. Os auditores podem examinar as políticas sem precisar estar na empresa, o que libera os recursos de TI que seriam usados por eles. Permitir que os auditores se mantenham atualizados sobre as alterações nas políticas por meio de arquivos exportados também permite um processo de conformidade mais tranquilo por identificar os possíveis problemas ainda no processo de preparação ao invés de quando estiverem em produção. Esse recurso também permite que as mudanças externas sejam importadas de volta ao BIG-IP ASM.



```
<?xml version="1.0" encoding="utf-8"?>
<policy name="phpauction_default" xmlns="http://www.f5.com/ASM/CP/policy">
  <encoding>utf-8</encoding>
  <web_application>phpauction</web_application>
  <maximum_http_length>8192</maximum_http_length>
  <maximum_cookie_length>8192</maximum_cookie_length>
  <description></description>
  <blocking>
    <enforcement_mode>transparent</enforcement_mode>
    <violation id="EVASION_DETECTED" name="Evasion technique detected">
      <alarm>true</alarm>
      <block>true</block>
      <learn>true</learn>
    </violation>
    <violation id="REQUEST_TOO_LONG" name="Request length exceeds defined
buffer size">
      <alarm>true</alarm>
      <block>true</block>
      <learn>true</learn>
    </violation>
  </blocking>
</policy>
```

Figura 3: Exemplo da política do BIG-IP ASM exportada para um formato XML legível para humanos.

## Opções de Integração

Aprimorar a integração com as outras soluções da F5 bem como com soluções de terceiros é extremamente importante para aplicar os aspectos de segurança com suavidade, sem impactar negativamente o desempenho das aplicações.

### Integração com o RamCache

O RamCache é usado geralmente nas plataformas BIG-IP para melhorar o desempenho e transferir o conteúdo acessado com frequência para um cache na memória. Usar cache de qualquer tipo pode ser problemático para a segurança da aplicação web pela falta de controle sobre ele e pela possibilidade de fornecer conteúdo em várias situações não autorizadas.

Uma integração mais profunda permite que o BIG-IP ASM v10.1 aproveite o RamCache para melhorar o desempenho sem sacrificar a segurança. O BIG-IP ASM v10.1 desativa automaticamente o uso do cache nas respostas bloqueadas e durante o uso do criador de política em tempo real. Além disso, o cache é limpo quando uma política nova é aplicada, garantindo que as políticas de segurança mais atuais afetem imediatamente as requisições e as respostas.



### **Cobertura melhorada com a integração WhiteHat**

O serviço Sentinel da WhiteHat Security é usado pelas organizações para fornecer uma avaliação contínua das vulnerabilidades das aplicações web. A integração da F5 com a WhiteHat Security permite que o Sentinel crie as políticas do BIG-IP ASM que previnem as vulnerabilidades descobertas pela verificação do WhiteHat Sentinel, dando o tempo necessário para que a TI e os desenvolvedores examinem, implementem e testem as correções dessas vulnerabilidades.

O BIG-IP ASM v10.1 melhora a integração já existente e agora permite que o WhiteHat Sentinel crie e aplique as políticas do BIG-IP ASM, que evitam outros métodos de ataques tais como:

- Injeção de comando
- Injeção de XPath
- Caminho transversal
- Divisão da resposta HTTP

## Conclusão

A segurança da aplicação web é um trabalho estressante com as constantes mudanças e a pressão cada vez mais difícil vinda de dentro e de fora da organização. A conformidade, o gerenciamento, os relatórios e essa porta giratória que são os vetores de ataque põem pressão sobre a infraestrutura e sobre os administradores, que precisam implementar as políticas de segurança para evitar o acesso não autorizado, bloquear os avassaladores ataques e ajustar constantemente as políticas conforme os novos usuários e aplicações.

A complexidade agregada resulta em uma segurança de aplicação web que é, na pior das hipóteses, incontrolável, e na melhor, difícil sem consideráveis investimentos em treinamento e experiência com produtos específicos.

O BIG-IP ASM v10.1 da F5 apresenta novos recursos planejados para melhorar a flexibilidade, ao mesmo tempo em que fornece o controle e a visibilidade necessários para os profissionais e administradores da segurança. Com essa nova versão, o BIG-IP ASM fornece capacidade de gerenciamento da segurança de aplicação web.

