



BIG-IP ASM Web Application Firewall Basic Concepts

PRESENTED BY:

Patrick Zoller, Systems Engineer

WE MAKE APPS  FASTER.
SMARTER.
SAFER.

Who is F5 Networks?



- Name inspired by the 1996 movie, *Twister*, in which reference was made to the fastest and most powerful tornado on the Fujita Scale: F5
- Based in Seattle USA, established in 1996, public in 1999, offices worldwide.
- Over 50% market share in Application Delivery Controller market.
- F5 Mission is to deliver the most secure, fast, and reliable applications to anyone anywhere, at anytime.
- 49 of Fortune 50 companies rely on F5
- Revenue US\$2.1 billion, no debt, 4,400 employees, Fortune 1000 company
- NASDAQ: FFIV

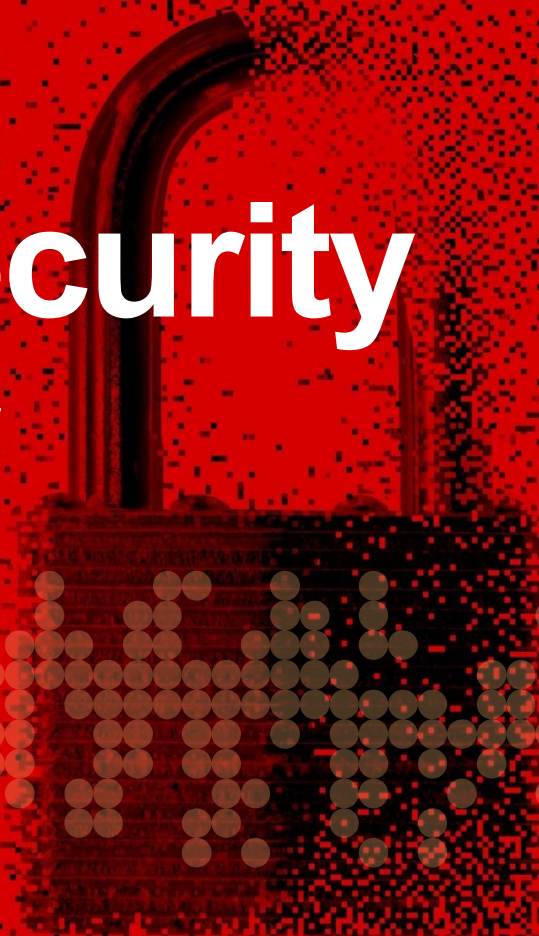
Who is F5 Networks?



Figure 1. Magic Quadrant for Web Application Firewalls



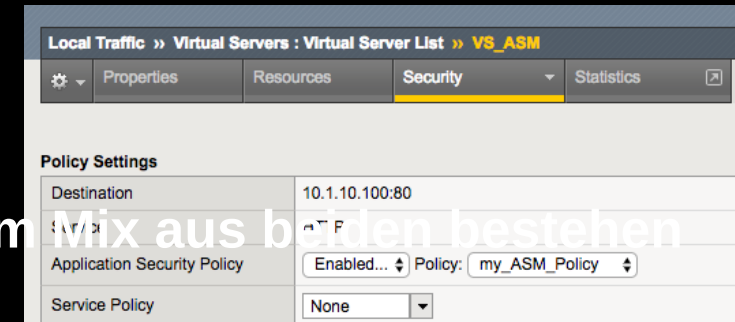
Application Security Manager



Application Security Policy 1/2

- Security Policies werden pro Applikation erstellt
- Policies können aus Negativ-, Positiv-Security und einem Mix aus beiden bestehen
- Optionen zum Erstellen einer Policy

- Manuell,
- Automatisch,
- DAST Integration:
 - HP Webinspect
 - IBM AppScan
 - ImmuniWeb
 - Qualys
 - Quantum Seeker
 - Trustwave App Scanner
 - GENERIC



Policy Building Settings

Security >> Application Security : Security Policies : Policies List

☆ Policies List Policy Groups Policies Summary Policy Diff

Create Policy Cancel Basic Advanced

On this screen you can configure policy settings for new policies and review policy settings for existing policies. Once a policy is configured, some settings on this page will have a link for editing the setting.

Policy Name	Policy Name...	Specifies the unique name of the policy.
	Partition: Common	
Description		Specifies an optional description of the policy. Type in any helpful details about the policy.
Policy Type	☒ Security ☐ Parent	Select a policy type: Security for an application security policy that you can apply to a virtual server, or Parent that you can use in order to attach Security policies to it, inheriting its attributes. Parent policies cannot be applied to Virtual Servers.
Policy Template	Fundamental	Choose a policy template for this policy.
Virtual Server	None	Select an Existing Virtual Server if you already configured one (An existing Virtual Server is displayed only if it has an HTTP Profile assigned to it and it is not using any Local Traffic Policy controlling ASM) and you would like to secure it, or New Virtual Server if you have not configured one, or None if you want to manually associate the newly created security policy to some virtual server at a later time.
Learning Mode	☒ Automatic ☐ Manual ☐ Disabled	Select how ASM handles the policy building process: Automatic will automatically accept learning suggestions once they reach 100%, Manual will require the administrator to accept every suggestion, and Disabled will cause that ASM does not create any learning suggestions. Note that an administrator can accept suggestions manually even in Automatic mode.
Enforcement Mode	☐ Transparent ☒ Blocking	Specifies how the system processes a request that triggers a security policy violation.
Application Language	Auto detect	Specifies the language encoding for the web application, which determines how the security policy processes the character sets.
Server Technologies	Select Server Technology...	Selecting one or more Server Technologies will add specific protections for the selected back-end server technology (for example, PHP will add attack signatures that cover known PHP vulnerabilities).
Trusted IP Addresses	IP Address / Netmask (optional) Add	In this area, you can specify IP addresses that the Policy Builder considers safe.
Policy Builder Learning Speed	☐ Slow ☒ Medium ☐ Fast	In this area you can view and change the conditions under which the Policy Builder adds or edits the security policy.
Signature Staging	☒ Enabled ☐ Disabled	Displays whether the signature staging feature is active.
Policy is Case Sensitive	☒ Enabled ☐ Disabled	Displays whether the security policy treats file types, URLs, and parameters as case sensitive (Enabled), or not (Disabled)
Differentiate between HTTP/WS and HTTPS/WSS URLs	☒ Enabled ☐ Disabled	Specifies, when enabled, that the security policy configures URLs specific to a protocol, meaning that the security policy differentiates between HTTP/WS and HTTPS/WSS URLs.

Application Security Policy 2/2

- Enforcement Modes: Transparent, Blocking
- Mode Blocking: Individuelle Funktionen können transparent bleiben
- Enforcement Mode in Abhängigkeit des Host Headers
- Policies können exportiert und importiert werden
- Policies können Hierarchien besitzen: Parent / Child Policies
- Policies können zwischen ASM Gruppen synchronisiert werden

The image displays three overlapping screenshots of the Application Security Policy management interface.

Top Screenshot: General Settings
Shows the 'Enforcement Mode' dropdown menu set to 'Transparent'. Below it, another 'General Settings' window shows the mode set to 'Blocking'.

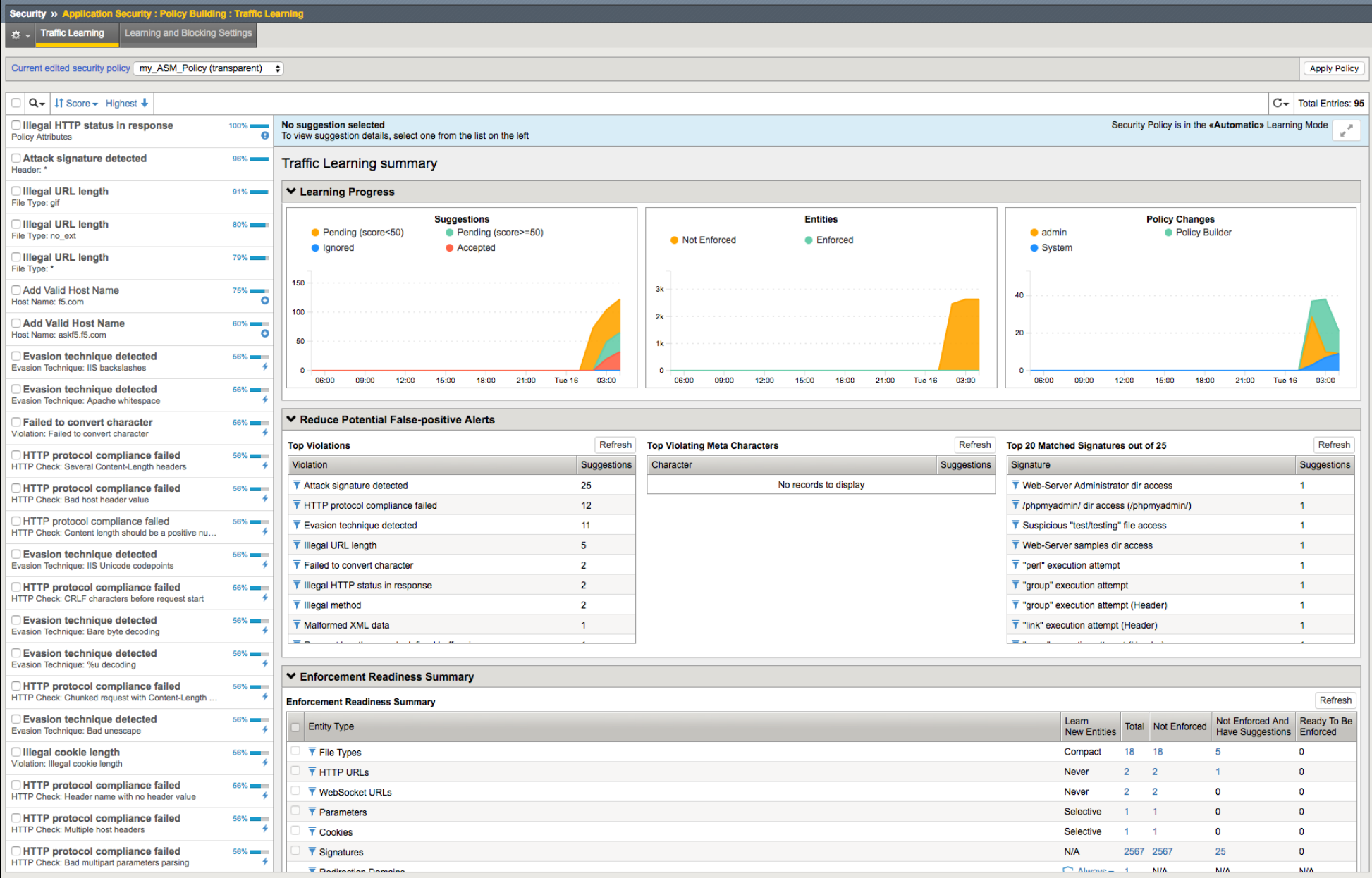
Middle Screenshot: Host Name Properties
Shows a list of policies on the left: 'my_parent' (selected, 0 child policies), 'my_ASM_Policy' (VS_ASM), and 'ASM_policy1'. On the right, the 'Policy Summary' section shows inheritance settings for various policy sections:

Policy Section	Inheritance
Attack Signatures	Mandatory Optional None
Custom Violations	Mandatory Optional None
Data Guard	Mandatory Optional None
Evasion Techniques	Mandatory Optional None
File Types	Mandatory Optional None
General Policy Settings	Mandatory Optional None

Bottom Screenshot: Synchronization
Shows the 'Application Security Synchronization' section with the following details:

Device Group	ASM-Productive	Warning: No synchronization will occur - Current device is the only member of the selected group
Device Group Members	/Common/bigipelk.itc.demo	
Device Group Type	Sync-Only	
Config Sync	Manual	

Traffic Learning 1/2



Traffic Learning 2/2

Security » Application Security : Policy Building : Traffic Learning

Traffic Learning

Learning and Blocking Settings

Current edited security policy

my_ASM_Policy (transparent)

Apply Policy

Q

Score

Highest

Total Entries: 95

Illegal HTTP status in response

Policy Attributes

100%

Accept Suggestion

Delete Suggestion

Ignore Suggestion

Related Suggestions

Attack signature detected

Header: *

96%

Action: Set URL Length to 128.

Matched File Type: gif

Illegal URL length

File Type: gif

91%

9 sample requests out of 27 that triggered the suggestion on 2018-01-16 04:04:59

Average Request Violation Rating 3.0

At least 9 untrusted sources / 0 trusted sources

Illegal URL length

Illegal URL length

File Type: no_ext

80%

[HTTP] /Portals/0/images/metapost/News-Articles/wa... 3

40.135.238.5

Illegal URL length [1]

Illegal URL length

File Type: *

79%

[HTTP] /weblogs/images/devcentral_f5_com/weblogs... 3

154.5.236.38

[HTTP] /weblogs/images/devcentral_f5_com/weblogs... 3

54.86.82.63

[HTTP] /weblogs/images/devcentral_f5_com/weblogs... 3

54.165.147.69

Geolocation

United States

Source IP Address

54.86.82.63:54552

Session ID

605622d89c0bebb5

Time

2018-01-16 03:42:49

Violation Rating

3

Request needs further examination

Attack Types

N/A

Add Valid Host Name

Host Name: f5.com

75%

[HTTP] /weblogs/images/devcentral_f5_com/weblogs... 3

54.86.82.63

Add Valid Host Name

Host Name: askf5.f5.com

60%

[HTTP] /weblogs/images/devcentral_f5_com/weblogs... 3

54.165.147.69

Evasion technique detected

Evasion Technique: IIS backslashes

56%

[HTTP] /weblogs/images/devcentral_f5_com/weblogs... 3

50.164.69.2

Evasion technique detected

Evasion Technique: Apache whitespace

56%

[HTTP] /weblogs/images/devcentral_f5_com/weblogs... 3

54.174.138.115

Failed to convert character

Violation: Failed to convert character

56%

[HTTP] /weblogs/images/devcentral_f5_com/weblogs... 3

37.77.117.139

HTTP protocol compliance failed

HTTP Check: Several Content-Length headers

56%

[HTTP] /weblogs/images/devcentral_f5_com/weblogs... 3

54.164.64.148

HTTP protocol compliance failed

HTTP Check: Bad host header value

56%

[HTTP] /weblogs/images/devcentral_f5_com/weblogs... 3

54.208.79.203

HTTP protocol compliance failed

HTTP Check: Content length should be a positive nu...

56%

Request

Response

Request actual size: 283 bytes.

HEAD /weblogs/images/devcentral_f5_com/weblogs/macvittie/WindowsLiveWriter/Infrastructure2.0TakesaHopForward_AA93/blockquote_thumb.gif

if HTTP/1.1

Host: devcentral.f5.com

X-Cnection: Close

X-Forwarded-For: 54.86.82.63

X-Forwarded-Port: 443

Connection: close

X-RETURN-CODE: 200

Central Policy Builder



F/P Example: Disable Signature on Parameter on URL

Security » Application Security : Parameters : Parameters List » Parameter Properties

Parameter Properties

Edit Parameter

Parameter Name	verzeichnis (Explicit)
Parameter Level	URL
URL Path	HTTP /myURL
Perform Staging	☒ Enabled
In Staging Since	2018-01-16 04:18:31
Last Staging Event Time	2018-01-16 04:18:31
Allow Empty Value	☒ Enabled
Allow Repeated Occurrences	☒ Enabled
Sensitive Parameter	☐ Enabled
Parameter Value Type	User-input value

Data Type Value Meta Characters Attack Signatures

☒ Check attack signatures on this parameter

Overridden Security Policy Settings:

Attack Signature	State
☐ Havij SQL Injection (Parameter)	Disabled
☐ iframe tag (Parameter)	Disabled

Global Security Policy Settings:

<<

>>

"%ALLUSERSPROFILE%" access (parameter)
"%APPDATA%" access (parameter)
"%CommonProgramFiles%" access (parameter)
"%COMPUTERNAME%" access (parameter)
"%COMSPEC%" access (parameter)
"%HOMEDRIVE%" access (parameter)
"%HOMEPATH%" access (parameter)
"%HOMESHARE%" access (parameter)
"%PROCESSOR_ARCHITECTURE%" access (parameter)
"%ProgramData%" access (parameter)

BIG-IP® ASM: Leadership in WAF

Traditional WAF

- Signatures (OWASP Top 10)
- DAST Integration
- Site Learning
- File/URL/Parameter/Header/Cookie Enforcement
- Protocol Enforcement
- Login Enforcement / Session Tracking
- Data Leak Prevention
- Flow Enforcement
- IP Blacklisting
- ...

Advanced WAF

- Bot Detection (incl. Mobile-Bot)
- Client Fingerprinting
- Session Hijacking
- Websocket Security
- Web Scraping Prevention
- Brute Force Mitigation
- Credential Stuffing
- L7 DDoS Protection
- Heavy URL Mitigation
- CAPTCHA Challenges
- HTTP Header Sanitization/Insertion
- Anti-CSRF Token Insertion
- Single Page Application
- PFS Ciphers

WE MAKE APPS



FASTER. SMARTER. SAFER.

