BIG-IP ASM
Web Application Firewall Basic Concepts

PRESENTED BY:

Patrick Zoller, Systems Engineer

WE MAKE APPS GO FASTER. SMARTER. SAFER.

© 2017 F5 Networks

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

© F5 Networks, Inc

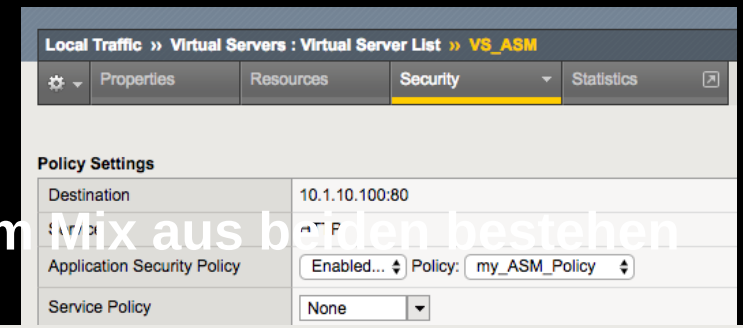
Who is F5 Networks?

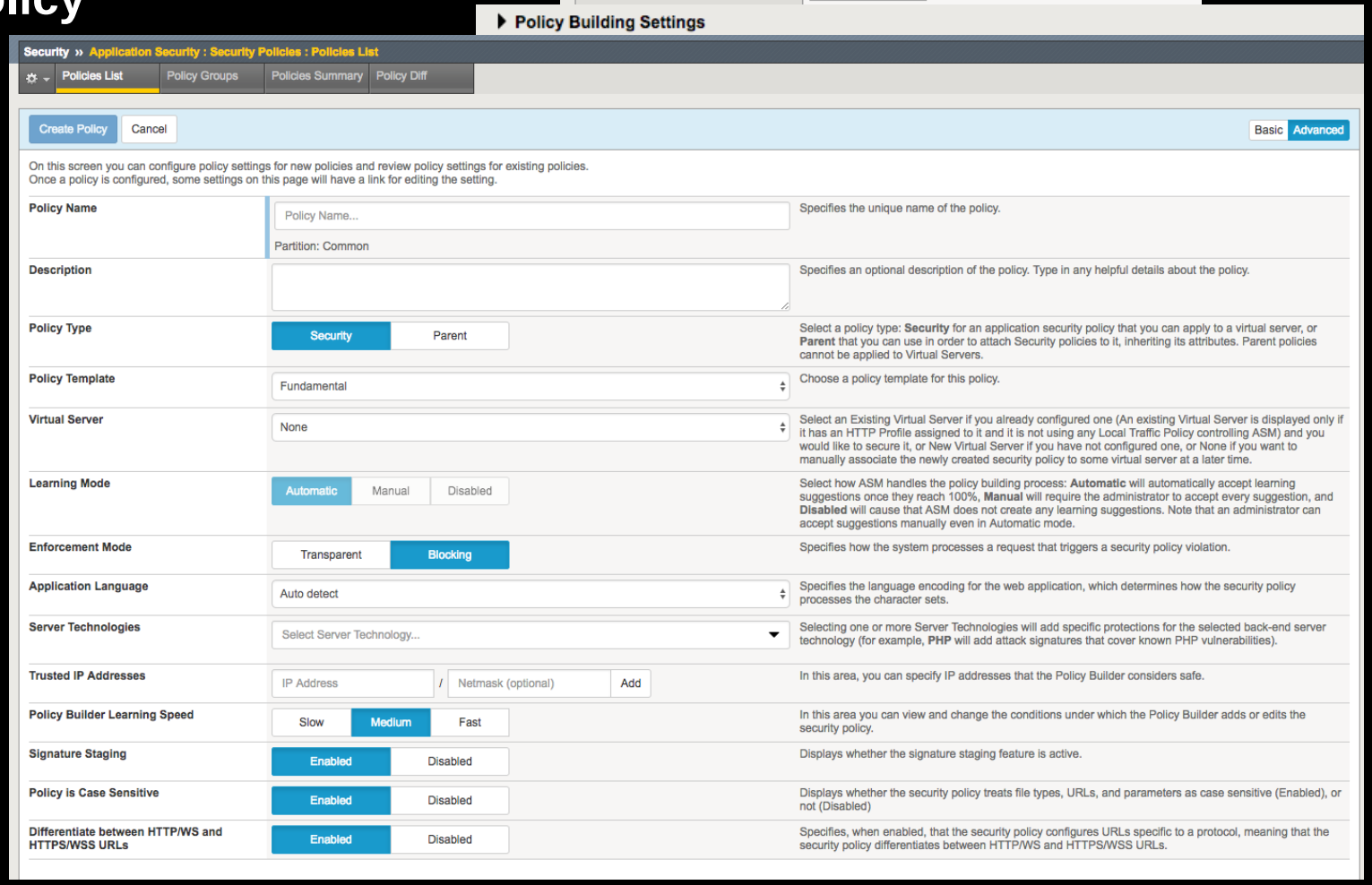
© F5 Networks, Inc

Application Security Manager

Application Security Policy 1/2

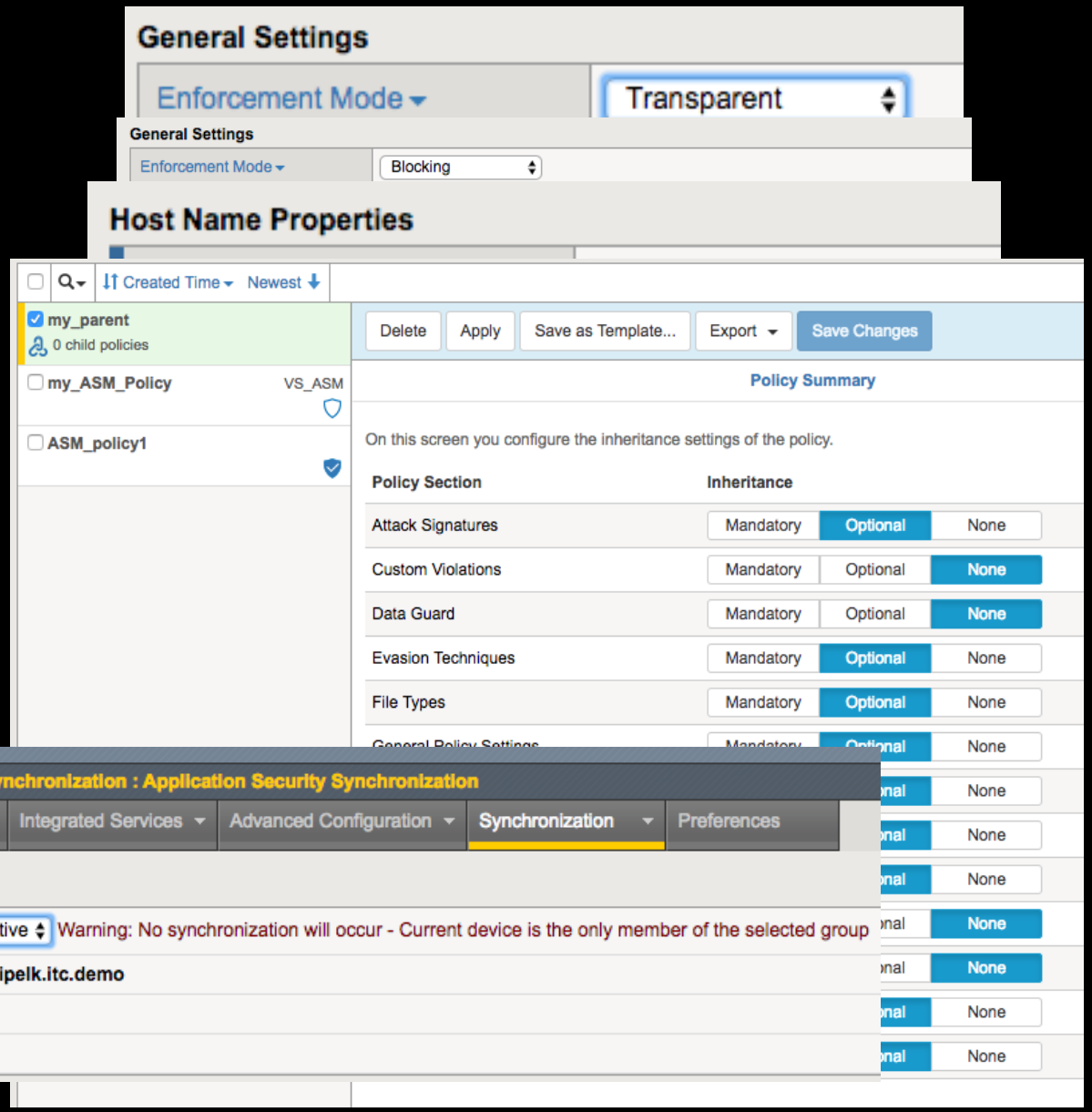
- Security Policies werden pro Applikation erstellt
- Policies können aus Negativ-, Positiv-Security und einem Mix aus beiden bestehen
- Optionen zum Erstellen einer Policy
  - Manuell,
  - Automatisch,
  - DAST Integration:
    - HP Webinspect
    - IBM AppSCan
    - ImmuniWeb
    - Qualys
    - Quantium Seeker
    - Trustwave App Scanner
    - GENERIC



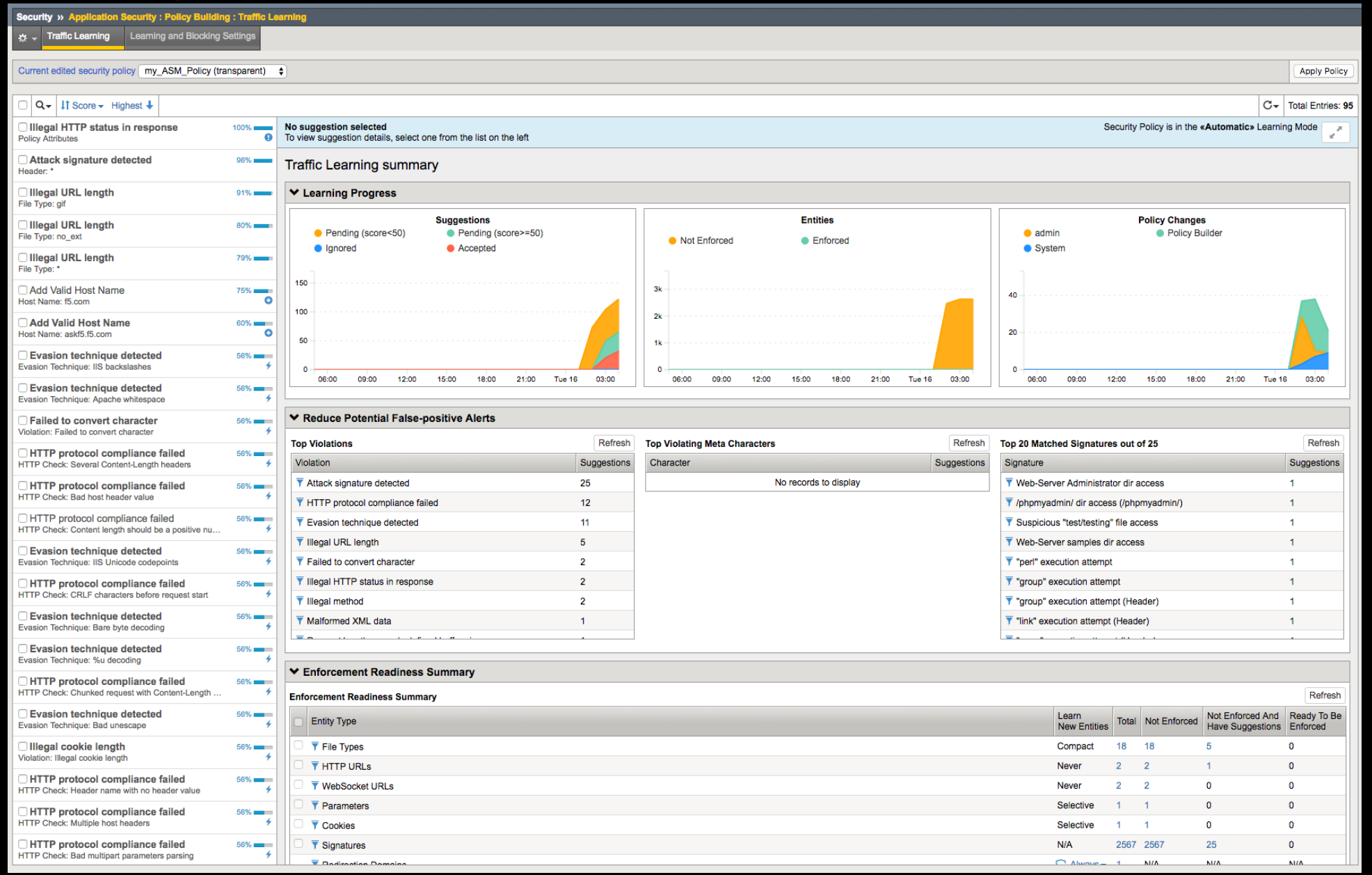


Application Security Policy 2/2

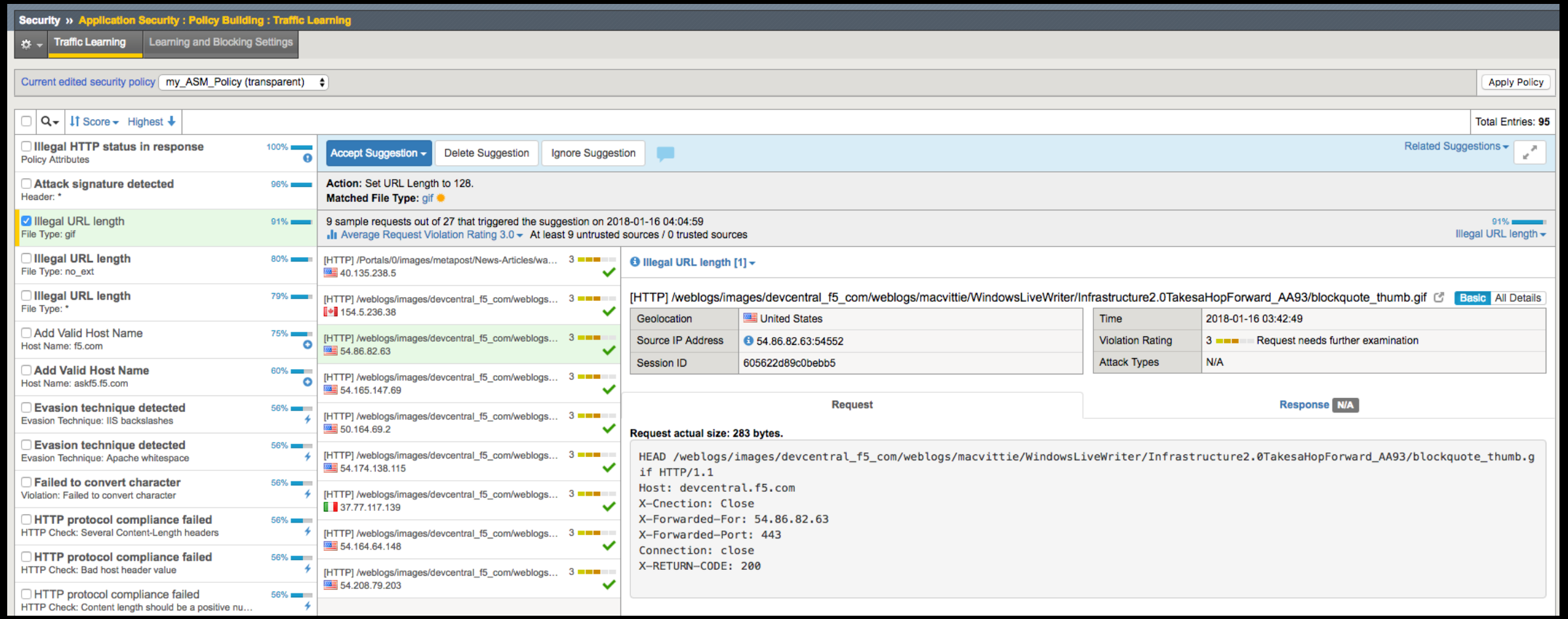
- Enforcement Modes: Transparent, Blocking
- Mode Blocking: Individuelle Funktionen können transparent bleiben
- Enforcement Mode in Abhängigkeit des Host Headers
- Policies können exportiert und importiert werden
- Policies können Hierarchien besitzen:
  Parent / Child Policies
- Policies können zwischen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



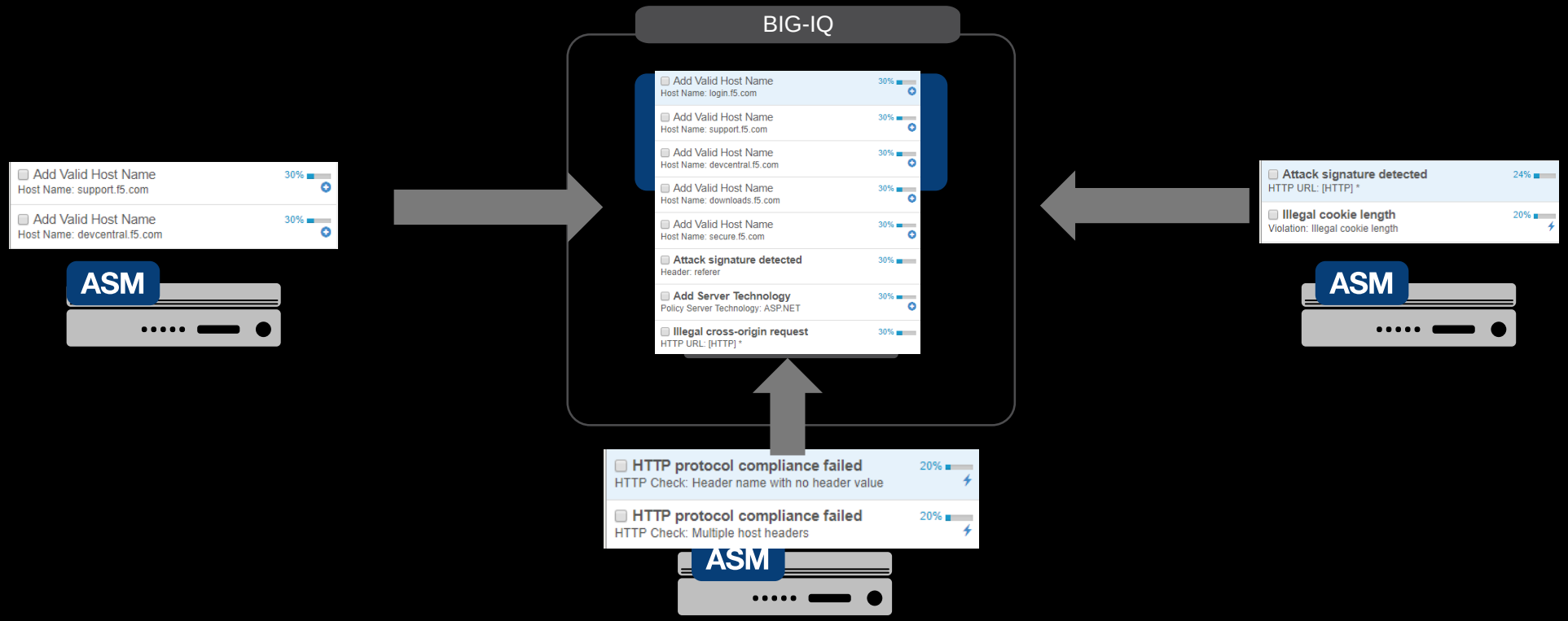
Traffic Learning 1/2



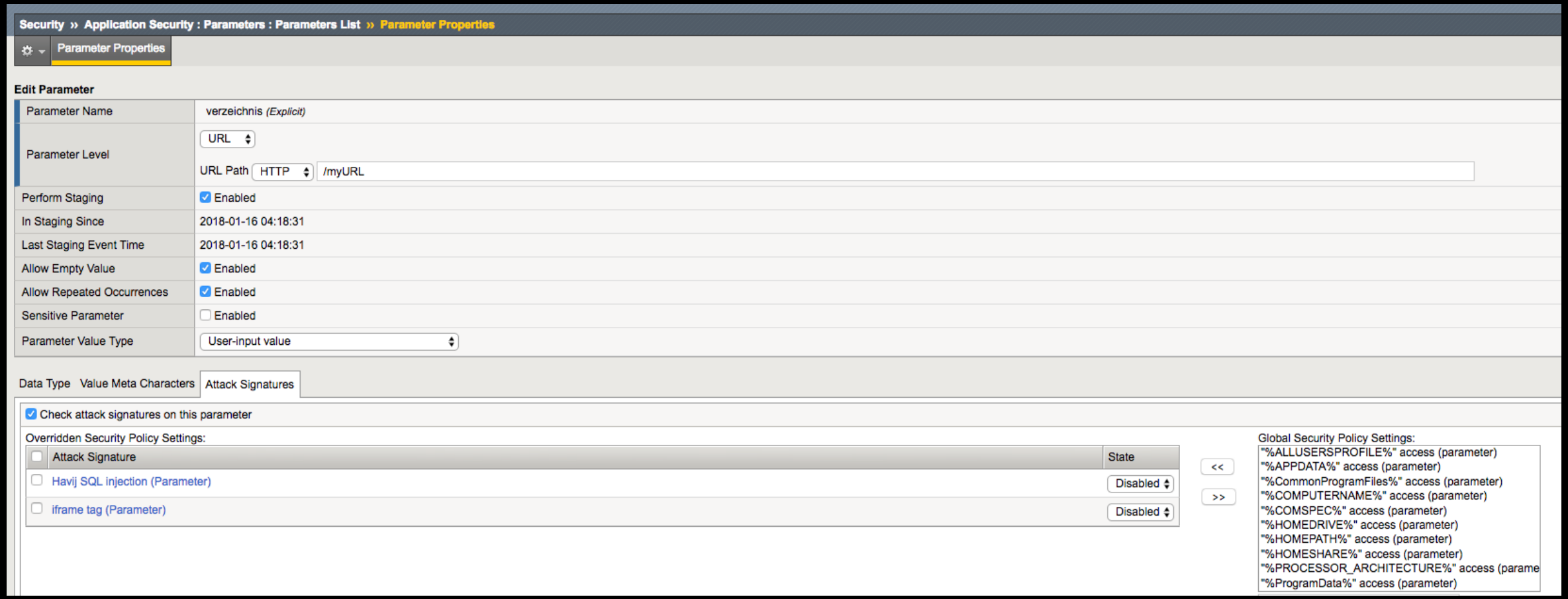
Traffic Learning 2/2



Central Policy Builder



F/P Example:
Disable Signature on Parameter on URL



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

© F5 Networks, Inc

WE MAKE APPS

FASTER. SMARTER. SAFER.