F5 - Optimalizácia prístupu a predovšetkým zabezpečenie štátnych elektronických portálových služieb

Jakub Šumpich, Territory Manager SEE

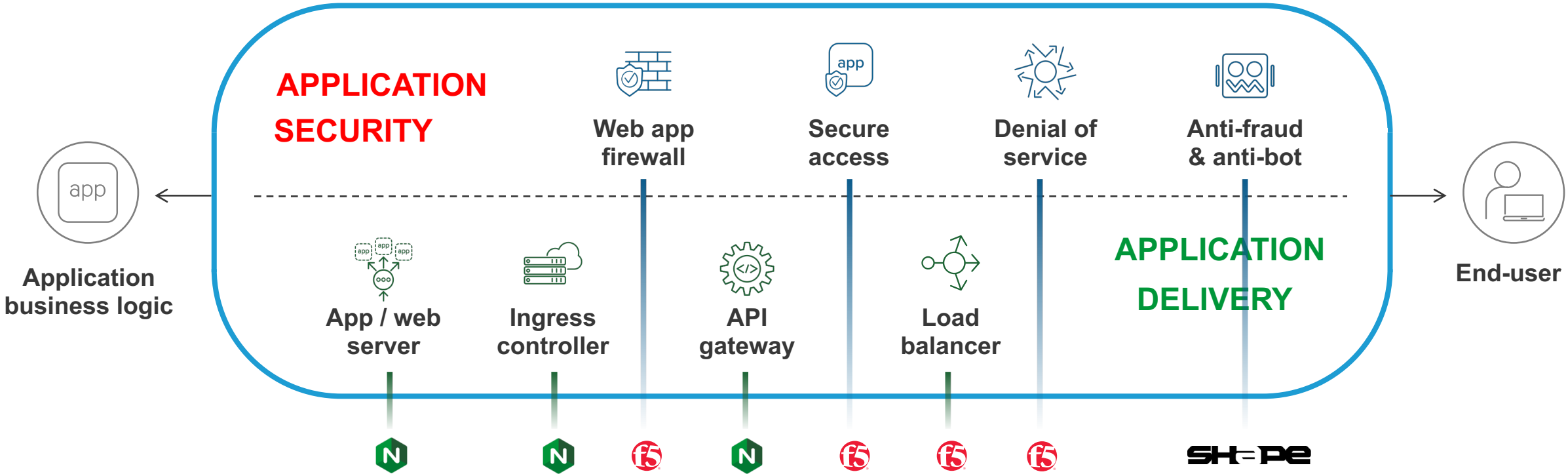
Email: J.Sumpich@f5.com

Kdo či Co je “F5”?

IT na začátku deploymentu nové aplikace

IT při provozu nové aplikace

Portfolio F5 nabízí na trhu to nejlepší z oblasti App Delivery s benefitem snížení komplexity a provozních nákladů



F5 je expert na L7/aplikační bezpečnost

Zákazníci v ČR a na Slovensku – více než 200 instalací

- Finance – Banky, nebankovní instituce, platební brány
- Komerční sektor – Sázkové kanceláře, utility, …
- Operátoři – Telco, ISP, poskytovatelé „manageovaných“ služeb
- Státní správa, kraje, velké státní podniky

MONETA UNIQA Tipsport O2 eset SKUPINA ČEZ SPCSS Státní pokladna Centrum sdílených služeb Správa informačních technologií Plzeň

Architektura, provoz a umístění aplikací se mění

Jak jsme byli zvyklí developovat aplikace

Jak nyní developujeme aplikace

Architektura, provoz a umístění aplikací se mění

RISE OF APIS FOR MICROSERVICES

86%

Enterprises that expect microservices to be the default application architecture in 5 years [1]

60%

Enterprises with microservices in pilot or production, citing agility and scalability as top motivators [2]

25%

Enterprises with over 1000 APIs, driven by the increased adoption of microservices [3]

1) https://lightstep.com/blog/microservices-trends-report-2018/
2) https://www.pingidentity.com/en/company/blog/posts/2018/security-and-it-professionals-concerned-about-enterprise-api-growth.html
3) https://www.globenewswire.com/news-release/2018/05/02/1494613/0/en/New-Research-Reveals-Record-Growth-in-Microservices-Is-Disrupting-the-Operational-Landscape.html

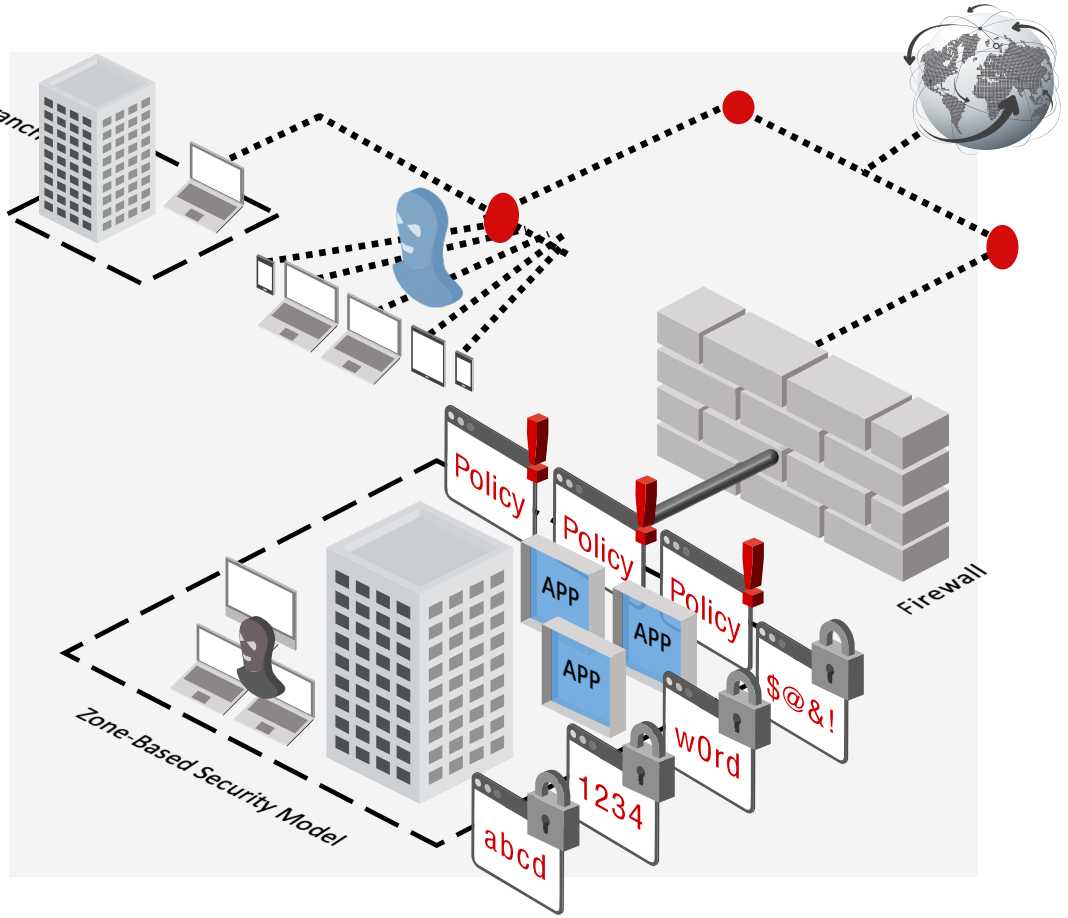
Mění se i struktura útoků

86% of internet threats target web servers

85% of websites has at least 1 vulnerability and an average of 56 per website

Prepare for application attacks every **15 minutes**

Millions of Bots actively attacking



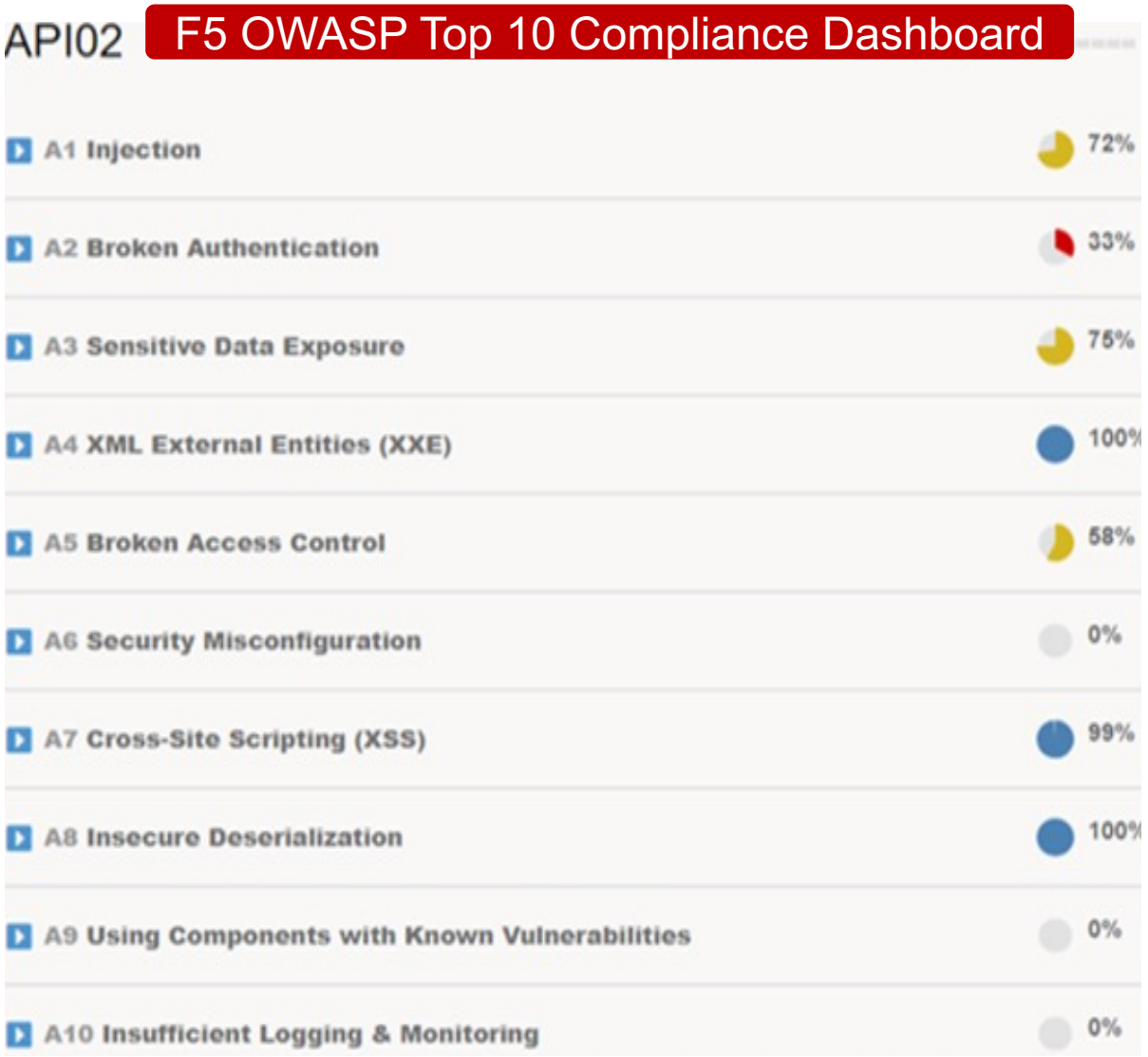
https://www.f5.com/labs/articles/threat-intelligence/how-cyber-attacks-changed-during-the-pandemic

Web developer with a job

Web developer without a job

OWASP
Open Web Application Security Project

- A broad consensus on the most critical web app flaws
- https://owasp.org/www-project-top-ten/
- Mitigation for well-known attack vectors that persist
- Coverage is a mandatory minimum for some regulatory requirements such as PCI DSS
- F5 complies with 2022 OWASP Top 10
- Beyond OWASP protection: bots, credential theft, app DoS, threat campaigns

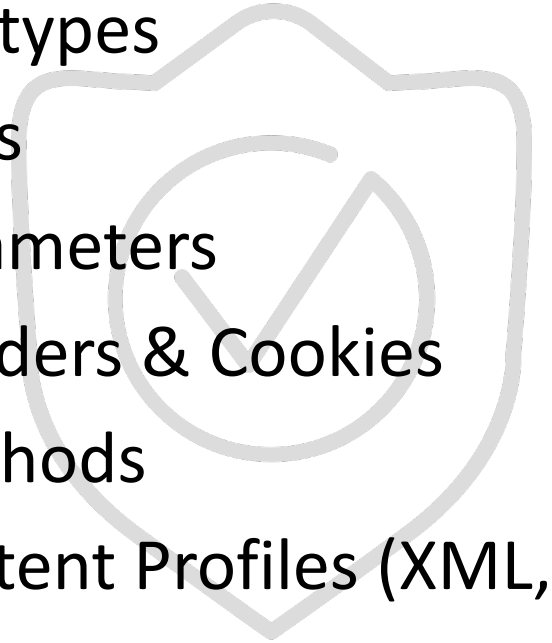


Co je a Proč “ WAF ”

WAF – Webový Aplikační Firewall

- **Negative Security**
  - Attack Signatures
  - Threat Campaigns
  - IP Intelligence

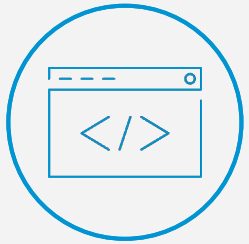
- **Positive Security**
  - File types
  - URLs
  - Parameters
  - Headers & Cookies
  - Methods
  - Content Profiles (XML, JSON…)



Traditional WAF

OWASP Top 10

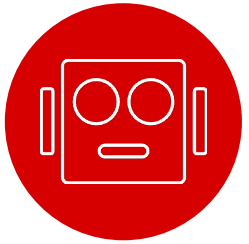
SSL/TLS Inspection



Scripting

F5 Advanced WAF

OWASP Top 10



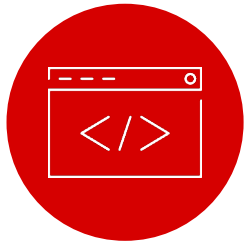
Proactive Bot Defense

Threat Campaigns

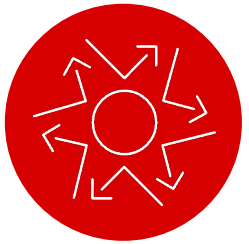
SSL/TLS Inspection

Credential Protection

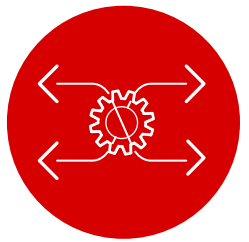
Credential Stuffing



Scripting



App-Layer DoS Protection



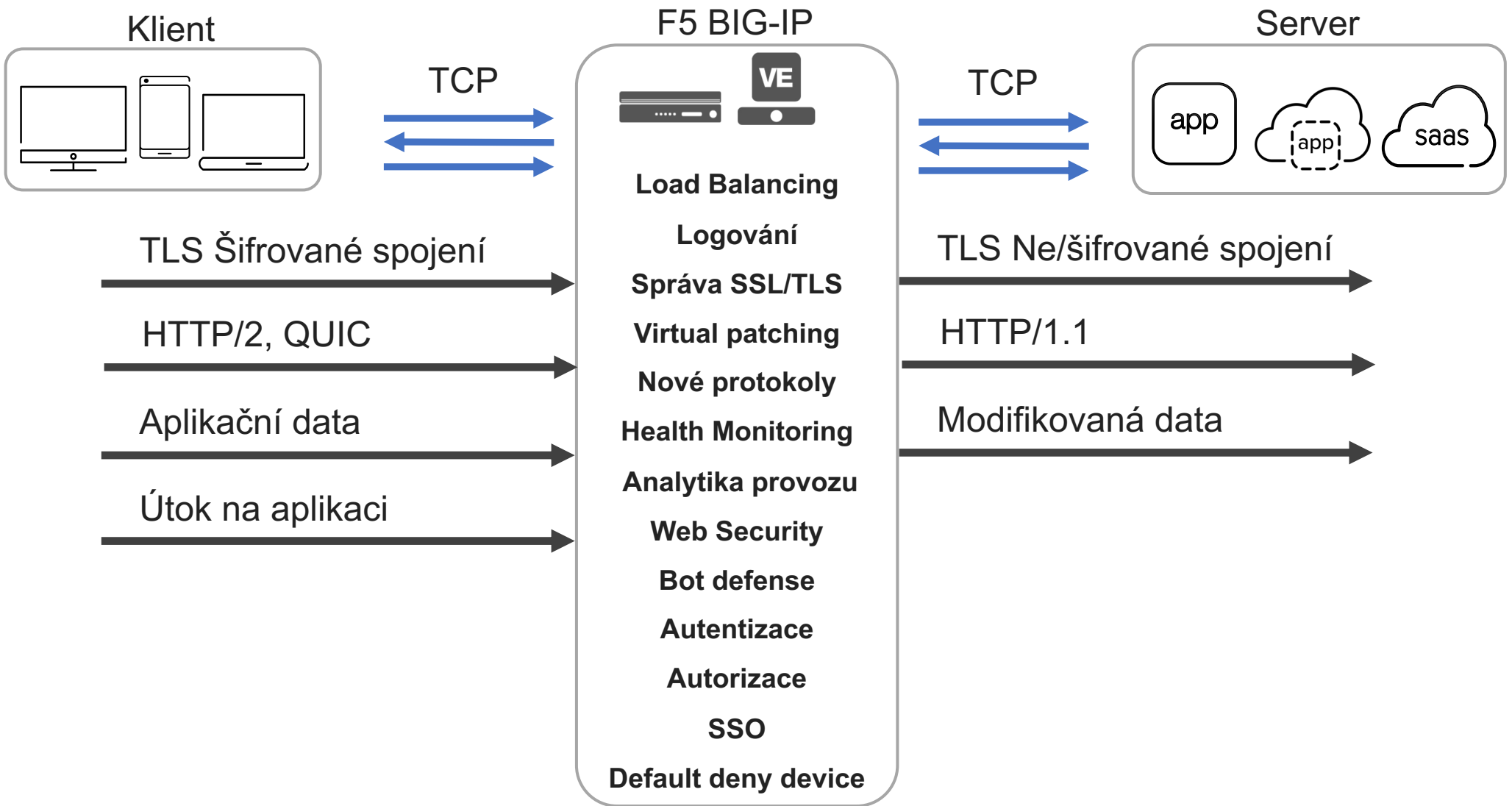
API Security

Co se změní implemetací WAF?

- Okamžitá eliminace TOP bezpečnostních problémů
- Vyšší viditelnost a schopnost předvídat útok
- Nezávislost na vývojovém týmu a verzích SW třetích stran
- Shoda v rámci ZoKB §20 ods. 3, ods. 4

F5 BIG-IP Full Proxy Architektura

- Kompletní oddělení klienstkého a serverového provozu



Případové studie

Use Case #1

PROVOZOVATEL PUBLIC IT SLUŽEB

- HW Platformy BIG IP, funcionality LB, WAF a FW/DDOS
- Publikuje přes 200 webů
- Nastavení WAF “všeobecným” způsobem, není uplná visibilita na Backend
- Funguje ochrana proti Brute Force útokům, kontrola "HTTP protocol compliance
- Jednoduché přiřazení Signatur pro konkretní URL/Parametr/Header
- Flexibilní Loggovaní – maskovaní hodnot citlivých parametrů, vypnutí posílání některých eventů do syslog
- Eliminace velkého množství útoků díky “IP Intelligence”

Use Case #2

IT ORGANIZACE MIFI

- HW Platformy BIG IP, “BEST” Bundle
- “ inteligentní” Geolokace – příklad:

k vybraným aplikacím je povolený přístup jen z vybraných zemí (např. V4)

- Let's Encrypt - automatické generovaní a vydávání SSL certifikátů
- APM - na autentifikaci uživatelů se využívá volaní RRP backendu (Gemalto)

přes SIDEBAND volání z F5 iRule (F5 scripting language) –
tímto způsobem je možno naintegrovat prakticky cokoli, co má API nebo WEB r.

- Úspěšná mitigace 3-4Gpbs DDOS útoku na Prezident.sk,

ve spolupráci s providerem (SWAN)

Use Case #3

PROVOZOVATEL “STATNIHO” CLOUDU

- HW Modulárni platformy F5 Viprion (škálovatelnost) BIG IP
- Separátni tenanty pro jednotlivé “zákazníky” (desítky)
- Zajišťení vysoké dostupnosti (modul LTM)
- Terminace SSL
- Globálni vysoká dostupnost a geolokace (modul DNS)
- Upgrade o WAF a AAA dodatečně v průběhu provozu

Funkce F5 *Loadbalanceru* a WAF “in 1 box”

- Vysoká dostupnost provozovaných aplikací
- Akcelerace aplikací
- Ochrana kritických aplikací v internetu a interní síti
- Single-sign-on, autentizační brána
- Eliminace nálezů z Penetračních Testů v aplikacích
- příp. DDoS, Anti-Bot ochrana

Podporujeme jakýkoli “ Use Case”

- HW Plarformy BIG IP a VELOS (On-Prem)
- BIG IP Virtual Edition (On-Prem, Cloud)
- As-A-Service

- Flexibilní licencování – Perpetual, Subscription, per “Consumption”

Největší výhoda – Silný lokální tým a podpora