



Případová studie nasazení F5 v SITMP Zabezpečený přístup k aplikacím & WAF

PRESENTED BY:

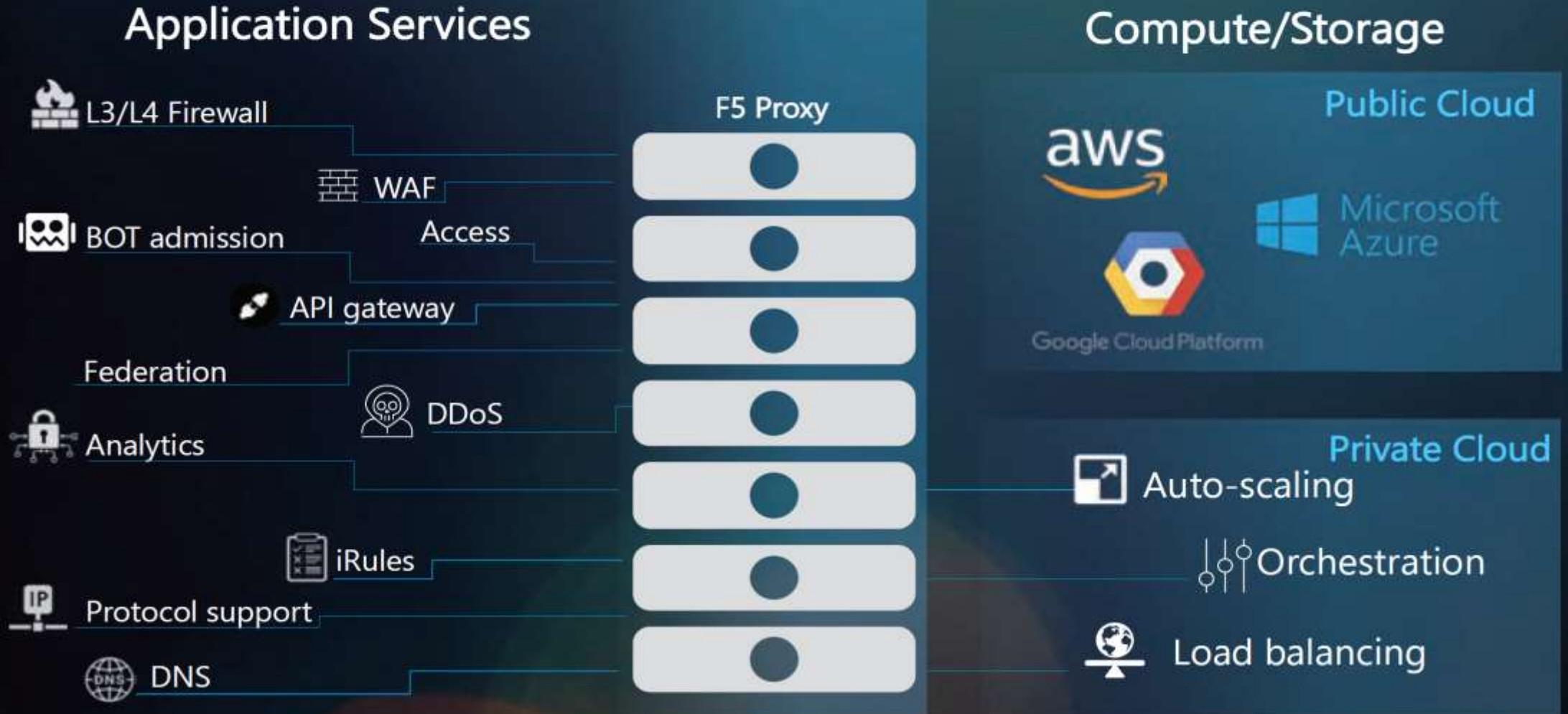
Martin Kylián - Network Security Engineer, Správa informačních technologií města Plzně

Filip Kolář – Account manager, Networks ČR

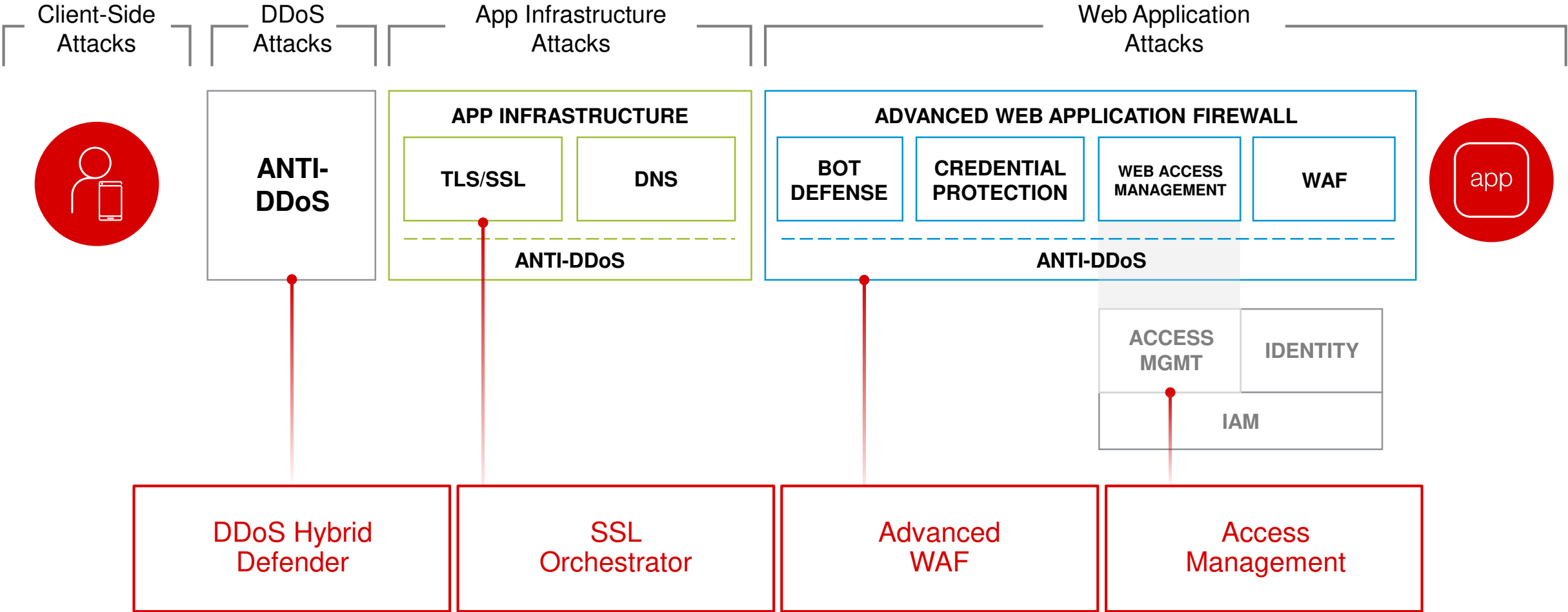
Radovan Gibala, Systémový inženýr, F5 Networks ČR

WE MAKE APPS  FASTER.
SMARTER.
SAFER.

F5 portfolio introduction



Complete App Protection Framework





Případová studie nasazení F5 v SITMP

Load Balancing, WAF, IAM

Kdo je to SITMP

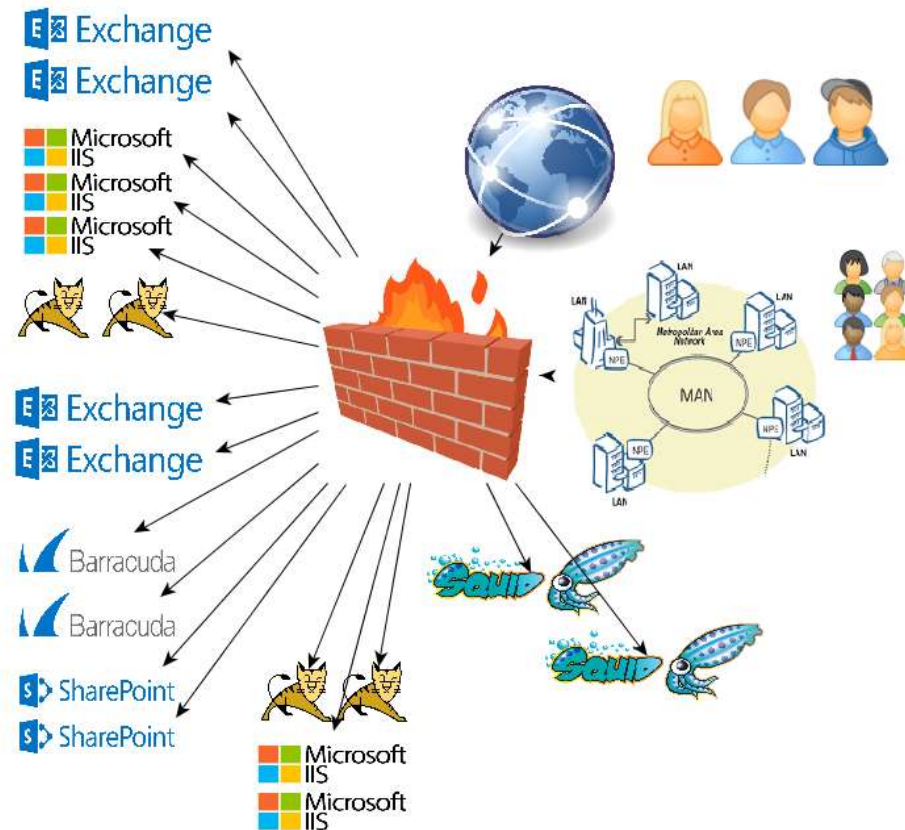
- IT pro ~100 organizací v Plzni
- 20.000 uživatelských identit
- Úřady
- Školy
- Sportovní areály...

Co zajišťujeme

- Výpočetní technika
- Metropolitní síť
- Datová centra
- Aplikace
- Procesy
- Kyberbezpečnost
- Vzdělávání

Kde jsme byli

- Několik Core služeb
- MS Exchange, MS Sharepoint
- Různé: webové servery a technologie, aplikace, správci



Cíl č.1 – vysoká dostupnost

- SMTP Gatewaye
- Exchange
- Škola on-line
- Http proxy

The screenshot displays the ŠKOLA ONLINE web application. The header features the 'd3' logo and the text 'ŠKOLA ONLINE'. The navigation menu includes 'Třídní kniha', 'Hodnocení', 'Výuka', 'Rozvrh a suplování', 'Evidence osob', 'Výstupy', and 'Komu'. The 'Hodnocení' menu is expanded, showing options like 'Zadávání hodnocení', 'Výpisy hodnocení', 'Uzávěrky', 'Slovní hodnocení', and 'Statistiky a přehledy'. The 'Výpisy hodnocení' sub-menu is further expanded to show 'Hodnocení žáka/studenta', 'Hodnocení v předmětu', and 'Hodnocení ve třídě'. Below the menu, there is a table with columns for 'Třída', 'Vyznamenáním', and 'Prospělo'. The table shows data for class '1.A' and a total row 'Celkem:'. At the bottom, there is a checkbox for 'Pouze aktivní k datu' with a date field set to '30.06.2017'.

Current Members

<input checked="" type="checkbox"/>	Status	Member
<input type="checkbox"/>	◆	skola1.plzen-edu.cz:80
<input type="checkbox"/>	●	skola2.plzen-edu.cz:80
<input type="checkbox"/>	●	skola3.plzen-edu.cz:80

Třída	Vyznamenáním	Prospělo
1.A	0	0
Celkem:	0	0

Pouze aktivní k datu *

Sekundární přínosy LB

- Centrální správa SSL certifikátů
- Centrální správa celého SSL stacku / offload SSL

Na co si dát pozor

- Stavové aplikace – persistence Sessions
- Správné url – wsdl, odkazy na assety...

Cíl č.2 – bezpečnost web aplikací

Klíčové vlastnosti

- OWASP top 10
- Ochrana přihlašovacích formulářů

Nejzranitelnější systémy

- Redakční systém bez podpory výrobce (~150 webů)
- Hostingové servery – WP, Joomla, Drupal

Portál občana

Portál občana

Město Plzeň Elektronické podání občana Domů | Kontakty | Nápověda

přihlásit nová registrace

Elektronické podání občana

Informace **Magistrát** Městské obvody Organizace

Magistrát města Plzně

- Oblast odpady
- Oblast archivu
- Oblast bytová
- Oblast dopravy
- Oblast majetková
- Oblast památkové péče
- Oblast prezentace a marketingu
- Oblast registru vozidel a řidičů**
- Oblast sociální
- Oblast správních činností
- Oblast stavebně správní

Magistrát

Magistrát města Plzně

Oblast registru vozidel a řidičů:

Informace o postupech řešení životních situací naleznete na webu města Plzně v kategorii Úřad - [vyřídte si na úřadu](#).

Název formuláře	Online	PDF	Soubor	Odkaz
Oznámení o ztrátě, odcizení, zničení ŘP, MŘP, PPZR	online	PDF		
Oznámení o ztrátě, zničení nebo odcizení tabulky s registrační značkou	online			WWW
Plná moc	online			
Vydání mezinárodního řidičského průkazu	online	PDF		
Vydání paměťové karty dílny		PDF		

WAF - když to funguje

SQL Inj

```
Accept-Language: cs-CZ,cs;q=0.9
Cookie: f5_cspm=1234; JSESSIONID=62557EBE1635B95075D98B64CC718A97; TS0118f59c=0144410629c113220bfa8974b56eecb9853a4ffc57bb6b86ee4e61172ec6ea520aae777ed38a82e66302f035fff90810c9c183c0cd95161e7046d962424e5947a641709d22; JSESSIONID=DFFC487E7408E2C0CCC4023A862F9C0C; tritius_sql_history=select * from user where id = 7||SELECT count(*) FROM table_column_config WHERE header_config_root = -1179 and name = 'workType' and hs_path like 'G3803'|SELECT count(*) FROM table_column_config WHERE header_config_root = -1179 and name = 'workType'|SELECT * FROM table_column_config WHERE header_config_root = -1179 and name = 'workType'|select count(*) from user to user group where user = 7|select * from user to user group where user = 7||select * from charge_history where reader = 60753||select * from charge_history where reader = 19676||select * from borrow_cycle where reader = 61394||; TS01b16c26=01444106292b83cbb09c32b07126700f6f8db7c00a0d5c68cc37905fcd80c426ac543747d2c929273cce4111dc23807ddb7e2bfe5b3da8acb09e4c05424bd568f31d1a60461186bf421ada36c9d1e25ab1ac759d
```

```
GET /irj/portal/anonymous?NavigationTarget=ROLES://portal_content/IUO/Role/IUO_Anonymni/Elektronick__pod_n_ob_ana_1/Elektronickpodnobana/ID_MESTSKE_OBVODY_PAGE&obvod=M03&oblast=stav UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL# HTTP/1.0
```

Logon form protection

Brute Force: Maximum login attempts are exceeded [1]

Mitigated Action	Alarm and Blocking Page
Username	Hhhhh
Detected Failed Logins / Threshold	4 / 3 (at the time of attack detection)
Detection Period	60 minutes
Maximum Prevention Duration	60 minutes
Applied Blocking Settings	Block Alarm

POST /_Admin/LogIN/Default.aspx?ReturnUrl=/_Admin HTTP/1.1

This question is for testing whether you are a human visitor and to prevent automated spam submission.



What code is in the image?

submit

Your support ID is: 10419132438721077370.

WAF – na co dbát při nasazení

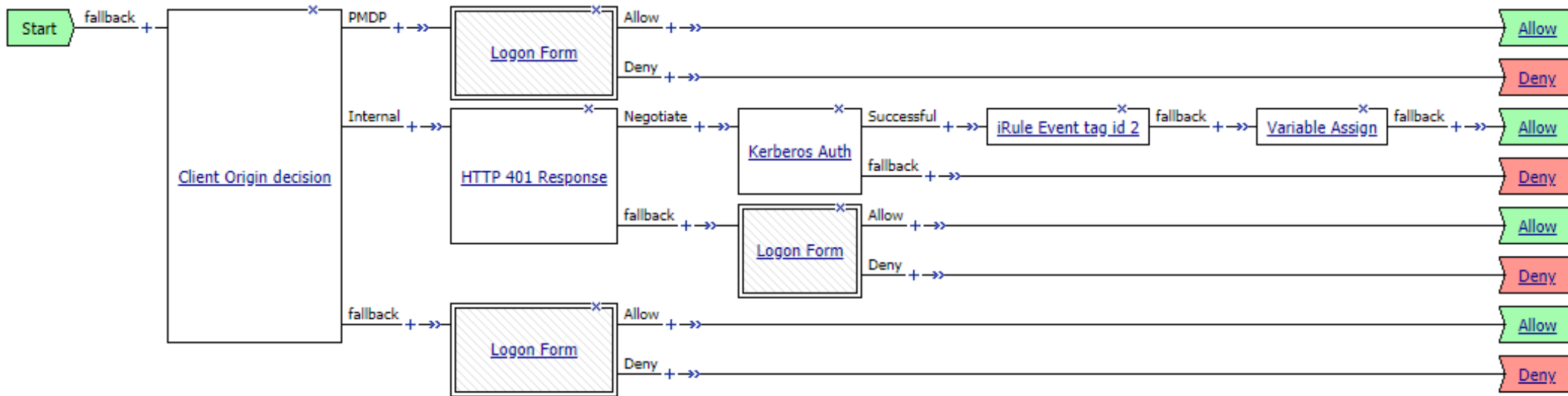
- Znalost aplikace nebo alespoň principů
- Cílit na přesné nastavení
- False pozitiva v negativním modelu / využívat staging
- Vše co nejlépe testovat

Cíl č.3 – identity access

Aplikace - chceme zpřístupnit, ale jen někomu

Naše další požadavky

- SSO
- Možnost řídit přístupové role
- Integrace s 2FA (připravujeme)



●	+	31383175	View	████████@PLZEN-CITY.CZ	192.168.90.78	/Common/VS_████████.plzen.eu	2019-03-28 10:52:02	2019-03-28 16:42:05	3890519	33879456	itm_apm
●	+	a26f9026	View	████████@PLZEN-CITY.CZ	192.168.90.57	/Common/VS_████████.eu_HTTPS	2019-03-28 14:39:55	2019-03-28 15:10:30	1025024	1838486	itm_apm
●	+	0a295465	View	████████	2a07:8d80:800:f17a:94f5:f3f3:8e37:9d37	/Common/VS_████████.plzen.eu_v6	2019-03-28 13:14:08	2019-03-28 17:15:55	122126	3091494	itm_apm
●	+	cbf215c4	View	████████@PLZEN-CITY.CZ	192.168.13.45	/Common/VS_████████.plzen.eu	2019-03-28 14:12:36	2019-03-28 18:13:02	100314	805443	itm_apm
●	+	faa29556	View	████████@PLZEN-CITY.CZ	192.168.90.116	/Common/VS_████████_HTTPS	2019-03-28 14:57:14	2019-03-28 15:27:35	225059	1049275	itm_apm
■	+	598e1d1e	View	n/a	54.37.23.163	/Common/VS_████████.plzen.eu	2019-03-28 14:54:49	2019-03-28 14:59:49	0	0	n/a
■	+	3df3c3fc	View	n/a	192.168.248.44	/Common/VS_████████_HTTPS	2019-03-28 14:57:40	2019-03-28 15:02:40	0	0	n/a
■	+	055a7933	View	n/a	54.37.22.123	/Common/VS_████████.plzen.eu	2019-03-28 14:53:10	2019-03-28 14:58:10	0	0	n/a



Obecné poznatky z nasazení

K nasazení f5 je potřeba

- Síťový specialista
- Aplikačního správce
- Bezpečnostního specialistu
- Programátora

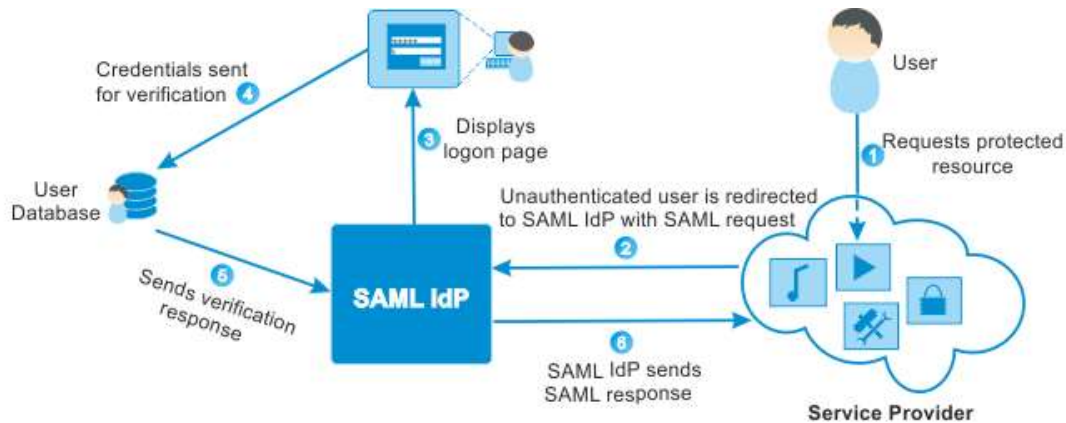
Shrnutí

Díky technologii f5 se nám podařilo

- Zajistit bezvýpadkový provoz
- Zabezpečit zranitelné aplikace
- Efektivně řídit přístupy k aplikacím

Kam dál?

- SAML IdP



Client-side Authentication Methods	Server-side Authentication Methods			
	HTTP Form	HTTP Basic	NTLM	Kerberos
HTTP Form	Yes	Yes	Yes	Yes
HTTP Basic	Yes	Yes	Yes	Yes
NTLM	No	No	No	Yes
Kerberos	No	No	No	Yes
Certificate	No	No	No	Yes
SAML ¹	Yes	Yes	Yes	Yes
RSA SecurID	No ²	No ²	No ²	No ²
One-Time Passcode	No ²	No ²	No ²	No ²

- Podpora kontejnerů

F5 Kubernetes BIG-IP Controller

F5 Kubernetes BIG-IP Controller manages F5 BIG-IP Local Traffic Manager (LTM) objects from Kubernetes.