ZJEDNODUŠENÍ SÍŤOVÉ BEZPEČNOSTI UVNITŘ DATOVÉHO CENTRA

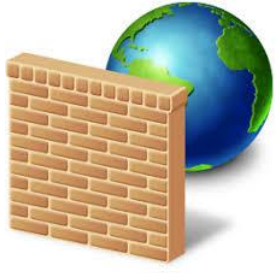
Jaroslav Sedláček | network architect

CONSULTING

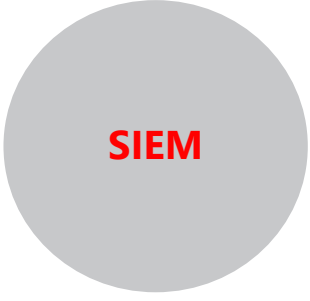
SÍŤOVÁ BEZPEČNOST UVNITŘ DATOVÉHO CENTRA

Firewall

IDS a IPS
Antimalware



WAF

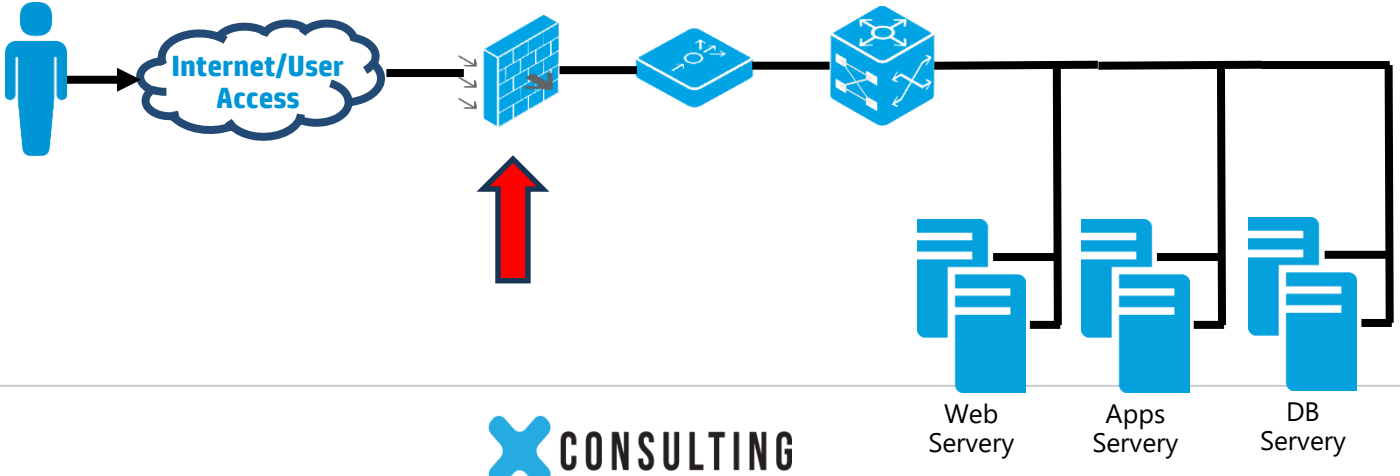


SIEM a log management

VYUŽITÍ FIREWALLU V DATOVÉM CENTRU

Perimeter firewall

- Filtrace provozu vstupujícího do DC
- Mnoho pokročilých funkcí
  - Integrované IPS
  - Rozpoznávání aplikací
  - Filtrování webového obsahu
- Ověřování uživatelů
- Zakončení VPN

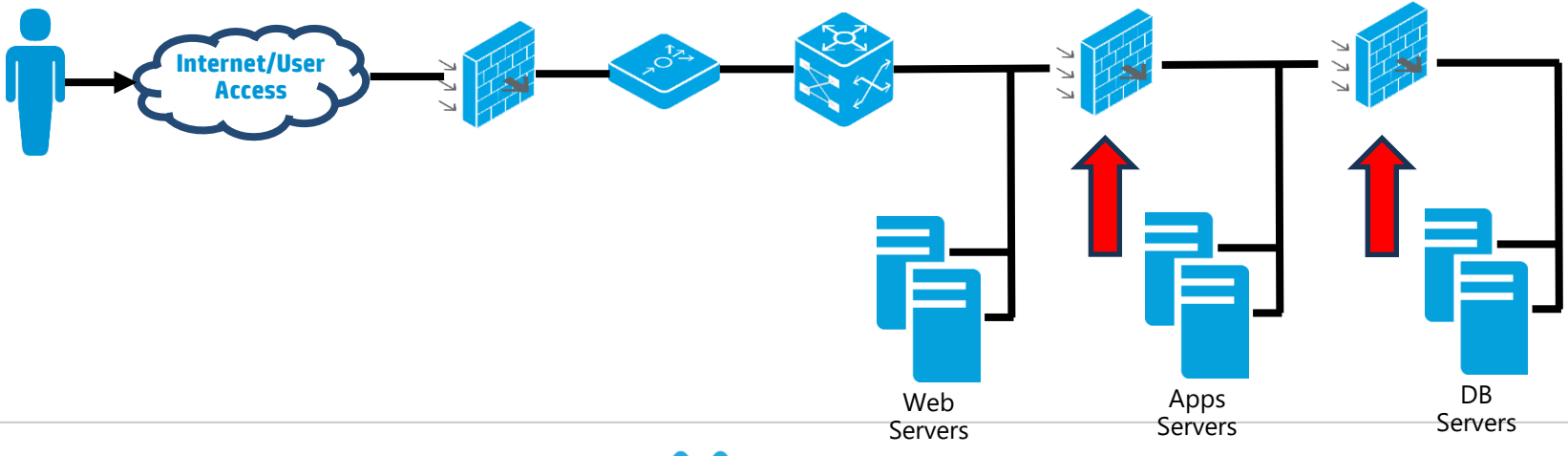


VYUŽITÍ FIREWALLU V DATOVÉM CENTRU

Segmentace uvnitř DC

- Stavová filtrace
- Definování TCP/IP prostupů mezi aplikacemi

- Omezí šíření útoku
- Oddělí bezpečnostní zóny
- Zajistí shodu se standardy
- Řídí komunikaci serverů s oddělenou správou

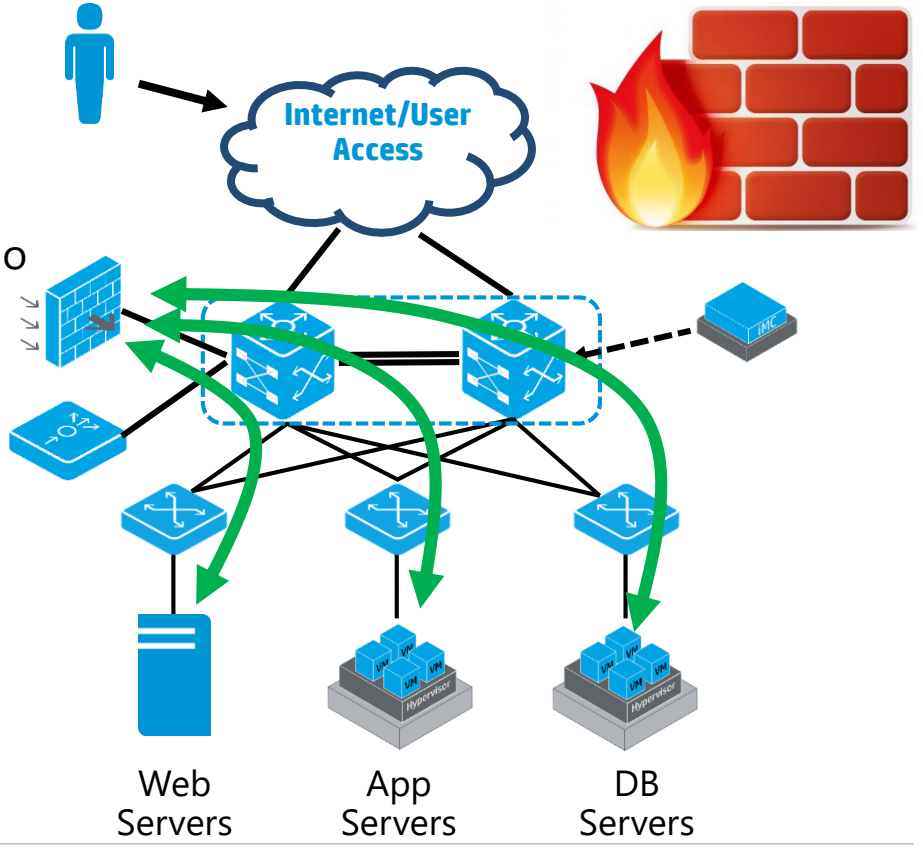


KLASICKÝ FIREWALL PŘI SEGMENTACI DC

Využití v DC

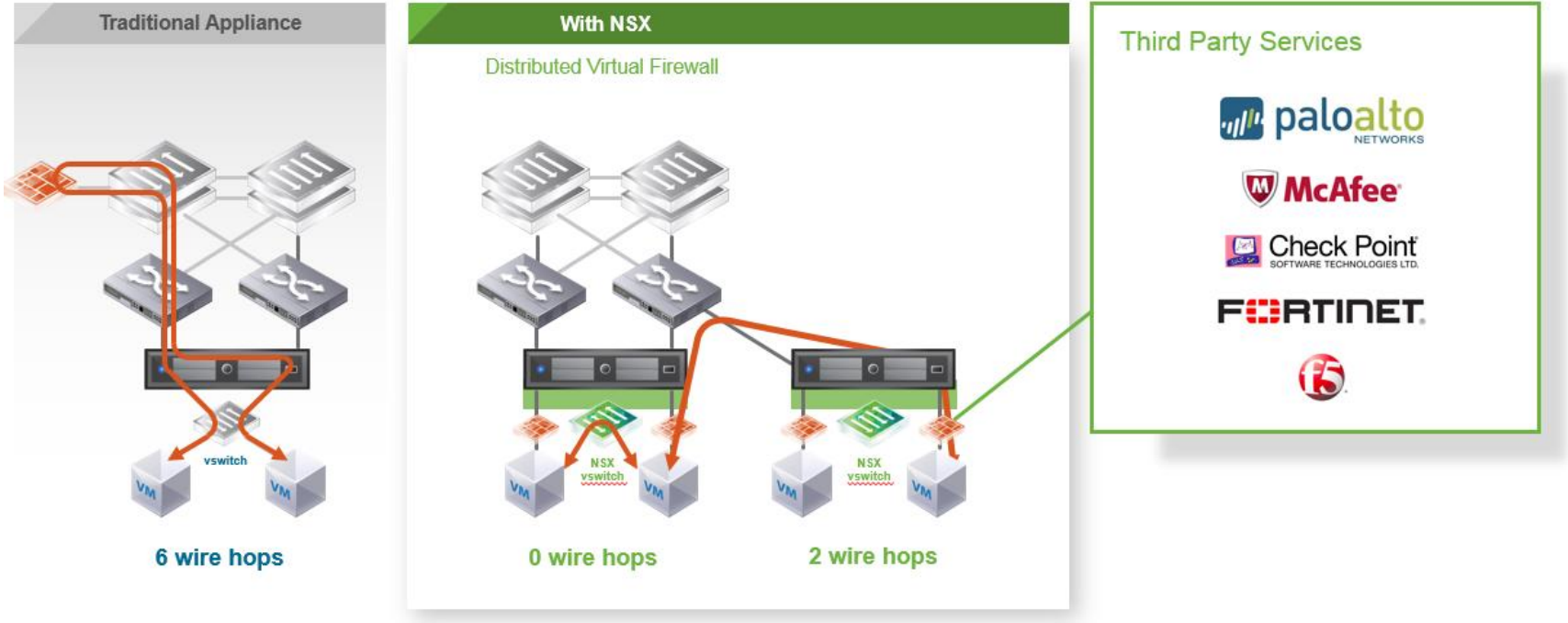
- Problém s výkonností
  - Vysoký podíl east-west provozu
- Firewall se stává úzkým hrdlem datového centra
- Správa DC firewallů je problematická a komplexní
- Pravidla pouze přibývají
- Je skutečně nutná stavová filtrace?

- Šetřete si výkon firewallu na skutečné bezpečnostní funkce!



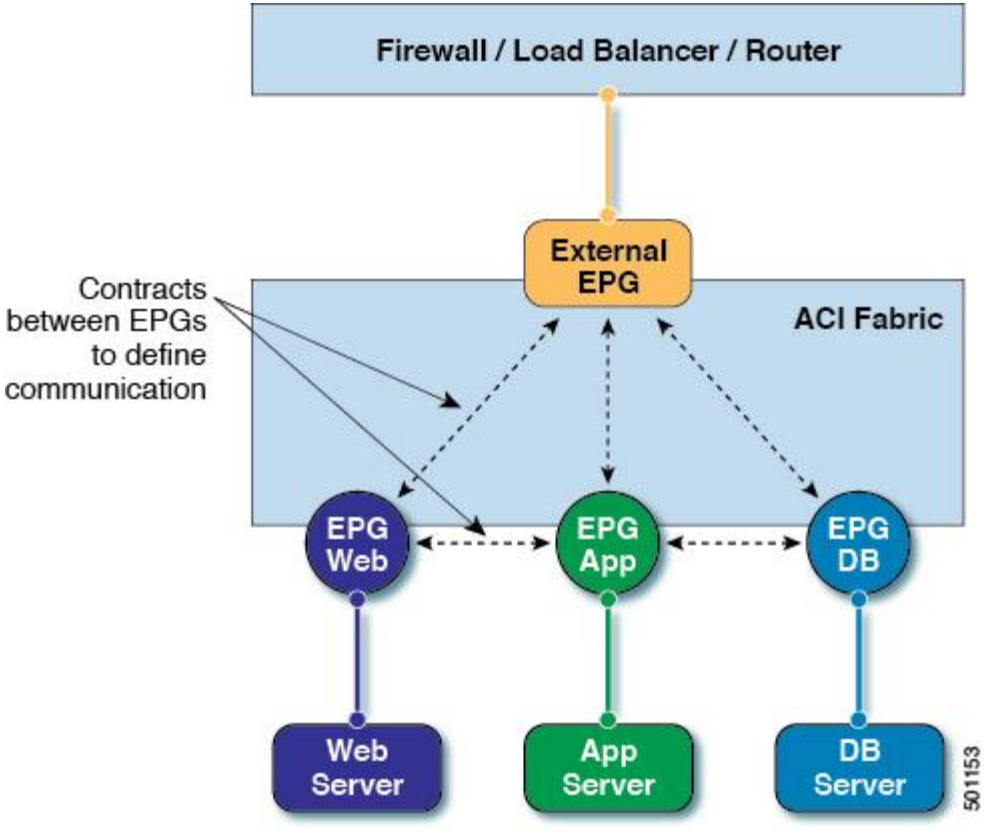
SDN
Software Defined Networking
v roli DC firewallu

NSX DISTRIBUOVANÝ FIREWALL



APPLICATION CENTRIC INFRASTRUCTURE

- Používá virtuální policy model
- Nastavení **kontraktů** mezi jednotlivými **EPG**
  - Kontraktem je filtr definující povolený provoz
  - EPG je slupina ekvivalentních konzumentů nebo poskytovatelů aplikace

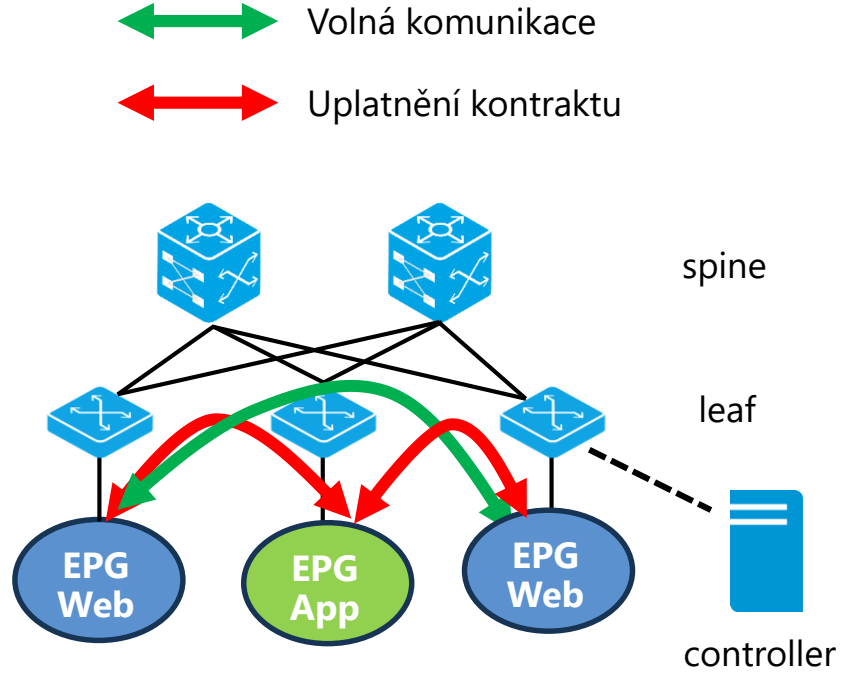


APPLICATION CENTRIC INFRASTRUCTURE

- Fyzická topologie leaf/spine
- Uplatnění kontraktu na vstupním leafu
  - Distribuované filtrování provozu
  - Centrální správa politiky (controller)

Kontrakt

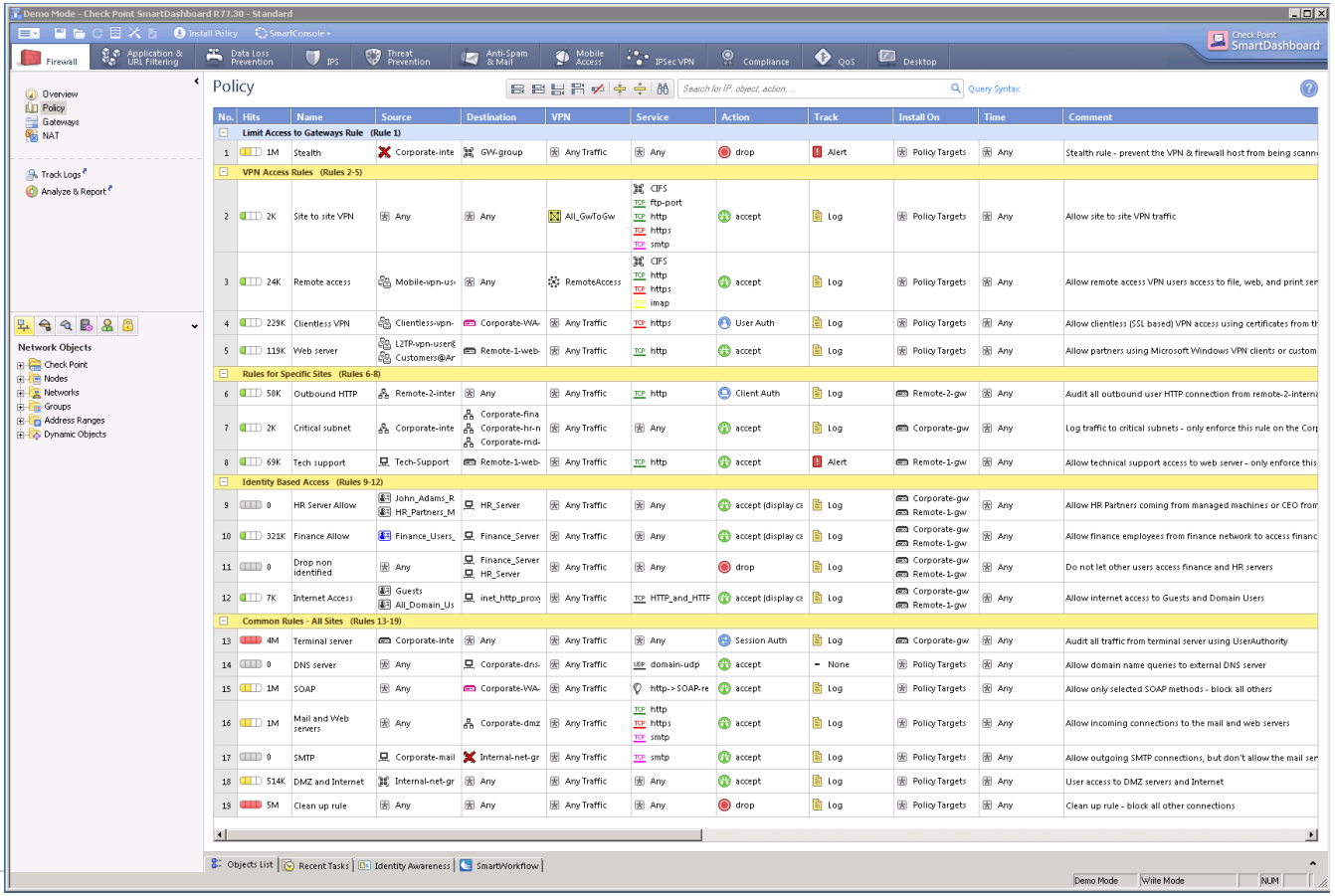
- Provider – poskytovatel aplikační služby
- Consumer – odběratel (zákazník) poskytované služby



A kde je ta automatizace ?

AUTOMATIZACE?

Takto to půjde obtížně



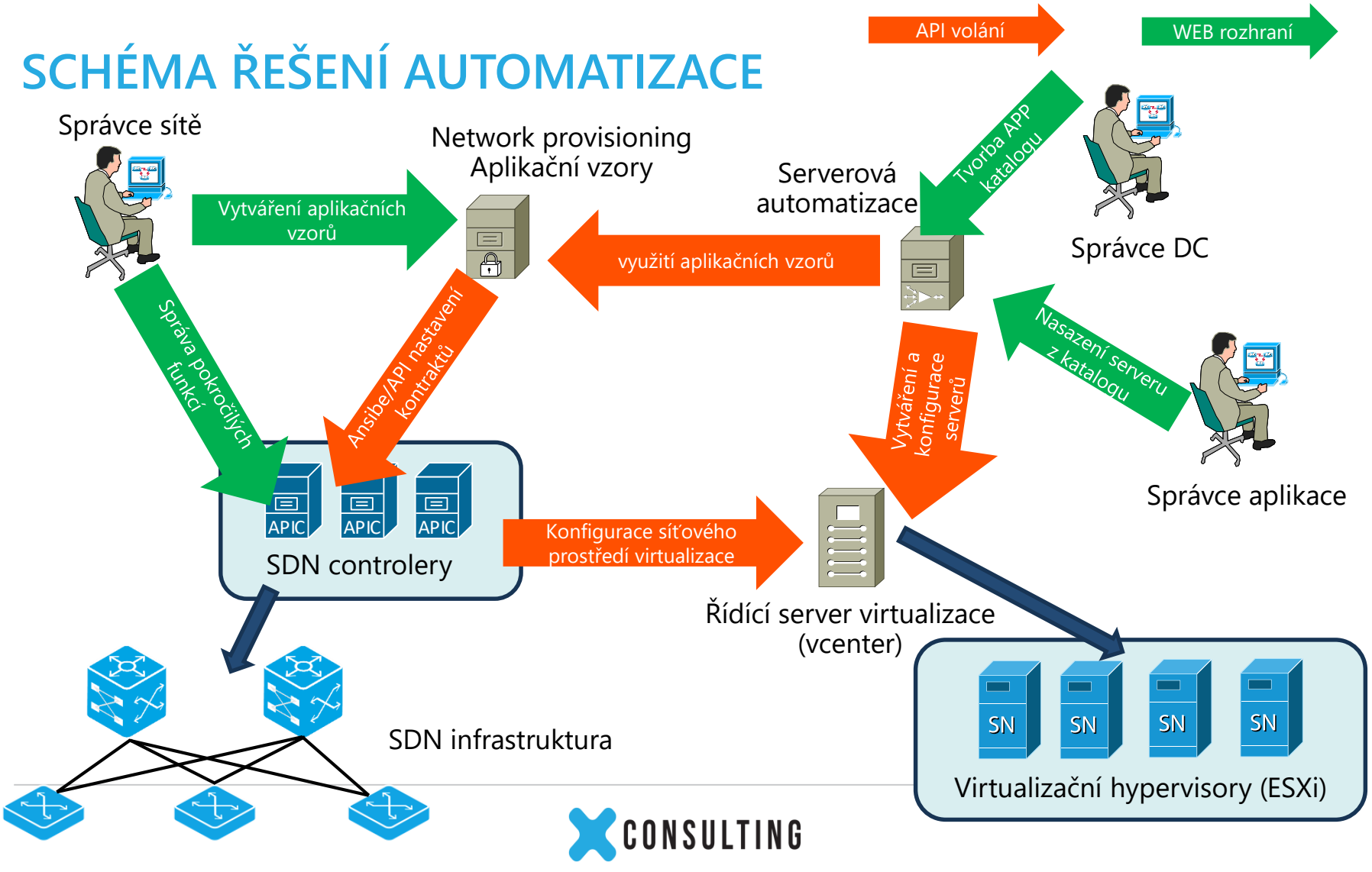
CONSULTING

AUTOMATIZACE FILTRAČNÍCH PRAVIDEL V DC

Co potřebujeme pro automatizaci

- **Definovat standardní pravidla** pro danou aplikaci
- Pomocí **API v SDN** infrastruktuře umožnit programové provádění konfiguračních změn
- Navázat bezpečnostní pravidla na **skupinu ekvivalentních** serverů (EPG/VLAN/Segment/Object-Group)
- Definovat set pravidel jako způsob **konzumace dané aplikace**
- **Aplikační katalog** svázat s pravidly pro aplikaci
- Pomocí serverové automatizace/orchestrace propojit nasazení aplikace s vytvořením filtračních pravidel

SCHÉMA ŘEŠENÍ AUTOMATIZACE



ZÁVĚR

Automatizace pravidel v DC

- Definovat **standardy** bezpečnostních pravidel
- Jasně zvolit metodologii kde bude filtrace uplatněna
- Sjednotit servery do ekvivalentních skupin

- Rozmyslet zda potřebuji firewall nebo mi stačí klasická filtrace
- Uzpůsobit infrastrukturu programovému řízení
- Použít automatizační nástroj na distribuci pravidel
- Nasadit firewall pro **pokročilé bezpečnostní funkce**

DĚKUJI ZA POZORNOST

Jaroslav Sedláček| network architect

@: jaroslav.sedlacek@xconsulting.cz

CONSULTING