

# ZJEDNODUŠENÍ SÍŤOVÉ BEZPEČNOSTI UVNITŘ DATOVÉHO CENTRA



**Jaroslav Sedláček** | network architect

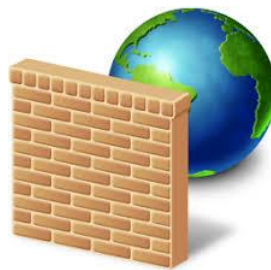
# SÍŤOVÁ BEZPEČNOST UVNITŘ DATOVÉHO CENTRA



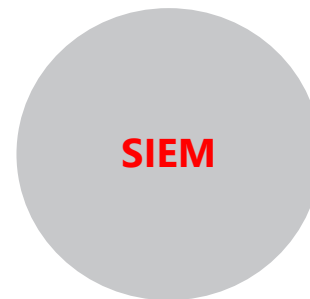
Firewall



IDS a IPS  
Antimalware



WAF

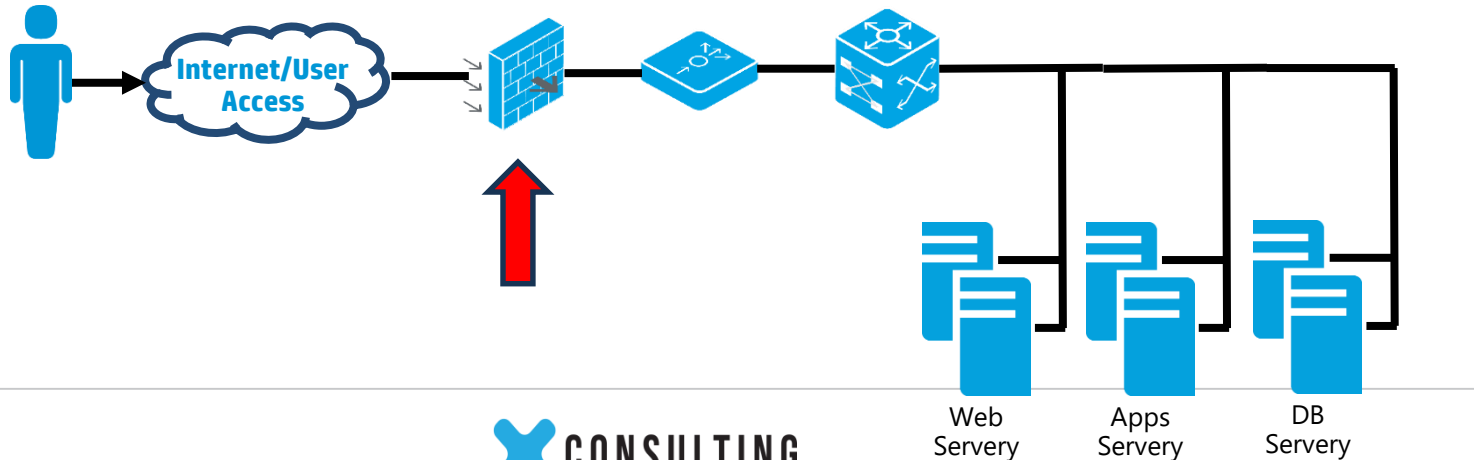


SIEM a log management

# VYUŽITÍ FIREWALLU V DATOVÉM CENTRU

## Perimeter firewall

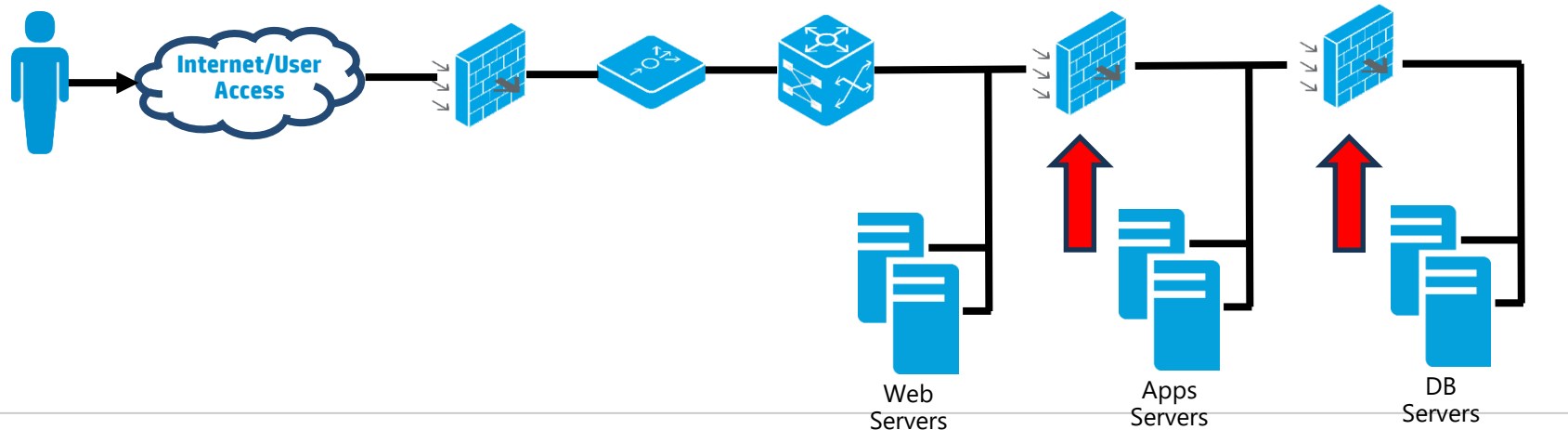
- Filtrace provozu vstupujícího do DC
- Mnoho pokročilých funkcí
  - Integrované IPS
  - Rozpoznávání aplikací
  - Filtrování webového obsahu
- Ověřování uživatelů
- Zakončení VPN



# VYUŽITÍ FIREWALLU V DATOVÉM CENTRU

## Segmentace uvnitř DC

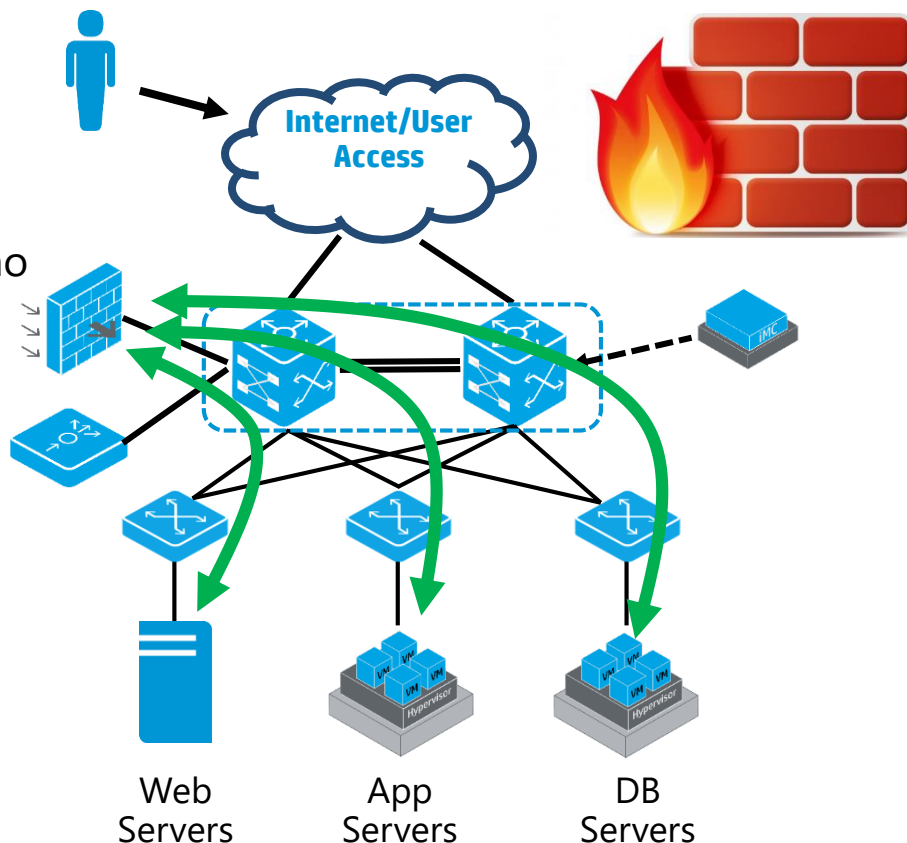
- Stavová filtrace
- Definování TCP/IP přístupů mezi aplikacemi
- Omezí šíření útoku
- Oddělí bezpečnostní zóny
- Zajistí shodu se standardy
- Řídí komunikaci serverů s oddělenou správou



# 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!



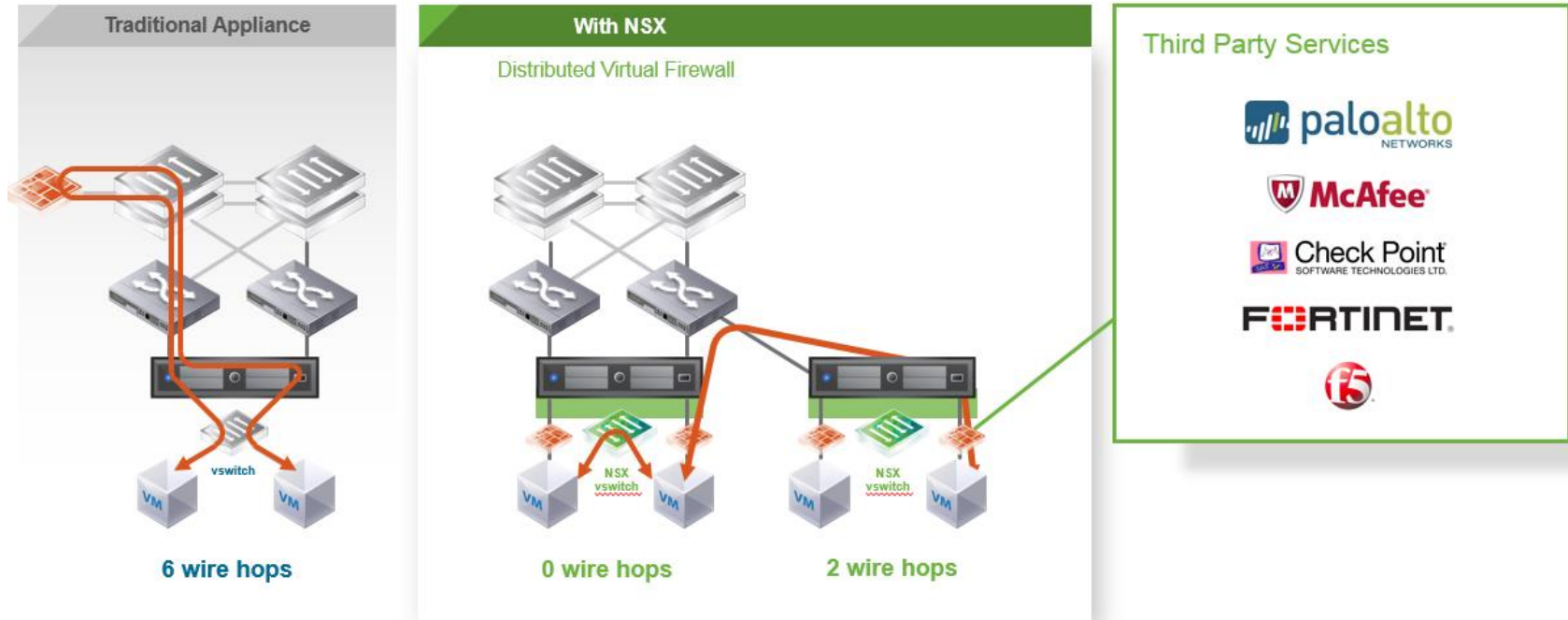
# SDN

## Software Defined Networking

### v roli DC firewallu

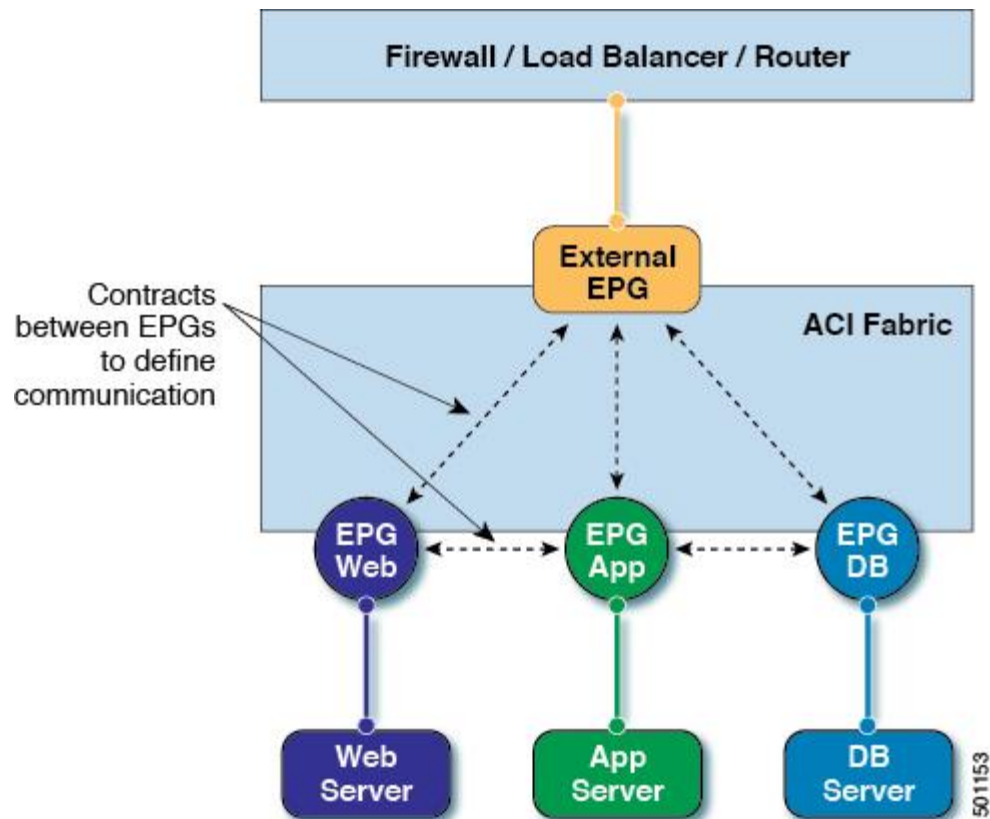


# NSX DISTRIBUTUOVANÝ FIREWALL



# APPLICATION CENTRIC INFRASTRUCTURE

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



501153

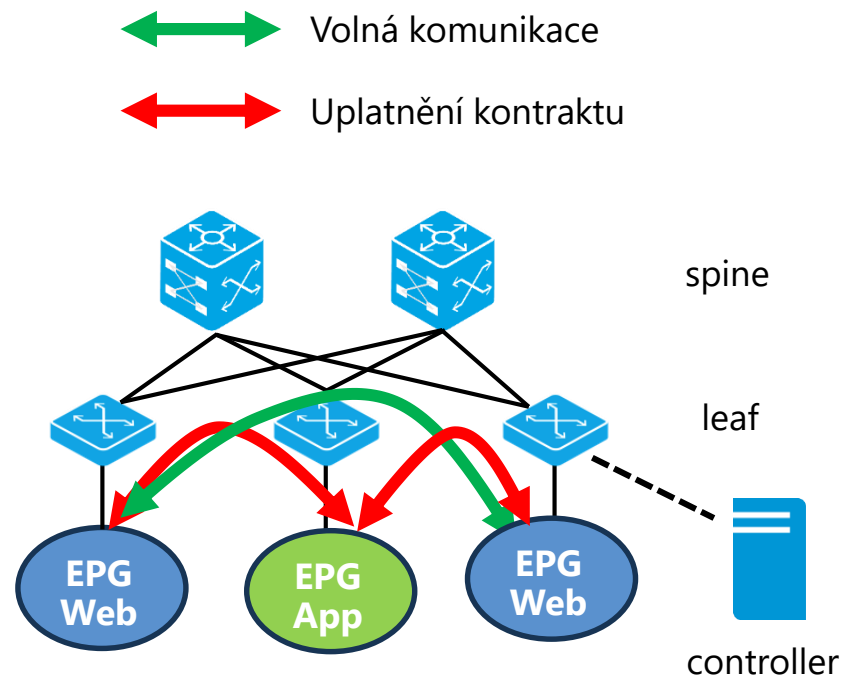


# APPLICATION CENTRIC INFRASTRUCTURE

- 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



Demio Mode - Check Point SmartDashboard R7.7.30 - Standard

Install Policy SmartConsole

Firewall Application & URL Filtering Data Loss Prevention IPS Threat Prevention Anti-Spam & Mail Mobile Access IPsec/VPN Compliance QoS Desktop

Check Point SmartDashboard

Policy

Search for IP, object, action...

Query Syntax

No.	Hits	Name	Source	Destination	VPN	Service	Action	Track	Install On	Time	Comment
<b>Limit Access to Gateways Rule (Rule 1)</b>											
1	1M	Stealth	Corporate-inte	GW-group	Any Traffic	Any	drop	Alert	Policy Targets	Any	Stealth rule - prevent the VPN & firewall host from being scanned
<b>VPN Access Rules (Rules 2-5)</b>											
2	2K	Site to site VPN	Any	Any	All_GwToGw	CIFS ftp-port http https smtp	accept	Log	Policy Targets	Any	Allow site to site VPN traffic
3	24K	Remote access	Mobile-vpn-us	Any	RemoteAccess	CIFS http https imap	accept	Log	Policy Targets	Any	Allow remote access VPN users access to file, web, and print ser
4	229K	Clientless VPN	Clientless-vpn-	Corporate-WA-	Any Traffic	https	User Auth	Log	Policy Targets	Any	Allow clientless (SSL based) VPN access using certificates from th
5	119K	Web server	L2TP-vpn-users@ Customers@Ar	Remote-1-web-	Any Traffic	http	accept	Log	Policy Targets	Any	Allow partners using Microsoft Windows VPN clients or custom
<b>Rules for Specific Sites (Rules 6-8)</b>											
6	58K	Outbound HTTP	Remote-2-inter	Any	Any Traffic	http	Client Auth	Log	Remote-2-gw	Any	Audit all outbound user HTTP connection from remote-2-intern
7	2K	Critical subnet	Corporate-inte	Corporate-fina Corporate-hi-n Corporate-md-	Any Traffic	Any	accept	Log	Corporate-gw	Any	Log traffic to critical subnets - only enforce this rule on the Corp
8	69K	Tech support	Tech-Support	Remote-1-web-	Any Traffic	http	accept	Alert	Remote-1-gw	Any	Allow technical support access to web server - only enforce this
<b>Identity Based Access (Rules 9-12)</b>											
9	0	HR Server Allow	John_Adams_R HR_Partners_M	HR_Server	Any Traffic	Any	accept (display c	Log	Corporate-gw Remote-1-gw	Any	Allow HR Partners coming from managed machines or CEO from
10	321K	Finance Allow	Finance_Users	Finance_Server	Any Traffic	Any	accept (display c	Log	Corporate-gw Remote-1-gw	Any	Allow finance employees from finance network to access financ
11	0	Drop non identified	Any	Finance_Server HR_Server	Any Traffic	Any	drop	Log	Corporate-gw Remote-1-gw	Any	Do not let other users access finance and HR servers
12	7K	Internet Access	Guests All_Domain_Us	inet_http_proo	Any Traffic	HTTP_and_HTTP	accept (display c	Log	Corporate-gw Remote-1-gw	Any	Allow internet access to Guests and Domain Users
<b>Common Rules - All Sites (Rules 13-19)</b>											
13	4M	Terminal server	Corporate-inte	Any	Any Traffic	Any	Session Auth	Log	Corporate-gw	Any	Audit all traffic from terminal server using UserAuthority
14	0	DNS server	Any	Corporate-dns-	Any Traffic	domain-udp	accept	None	Policy Targets	Any	Allow domain name queries to external DNS server
15	1M	SOAP	Any	Corporate-WA-	Any Traffic	http->SOAP-re	accept	Log	Policy Targets	Any	Allow only selected SOAP methods - block all others
16	1M	Mail and Web servers	Any	Corporate-dmz	Any Traffic	http https smtp	accept	Log	Policy Targets	Any	Allow incoming connections to the mail and web servers
17	0	SMTP	Corporate-mail	Internal-net-gr	Any Traffic	smtp	accept	Log	Policy Targets	Any	Allow outgoing SMTP connections, but don't allow the mail ser
18	514K	DMZ and Internet	Internal-net-gr	Any	Any Traffic	Any	accept	Log	Policy Targets	Any	User access to DMZ servers and Internet
19	5M	Clean up rule	Any	Any	Any Traffic	Any	drop	Log	Policy Targets	Any	Clean up rule - block all other connections

Objects List Recent Tasks Identity Awareness SmartWorkflow

Demio Mode Write Mode NUM

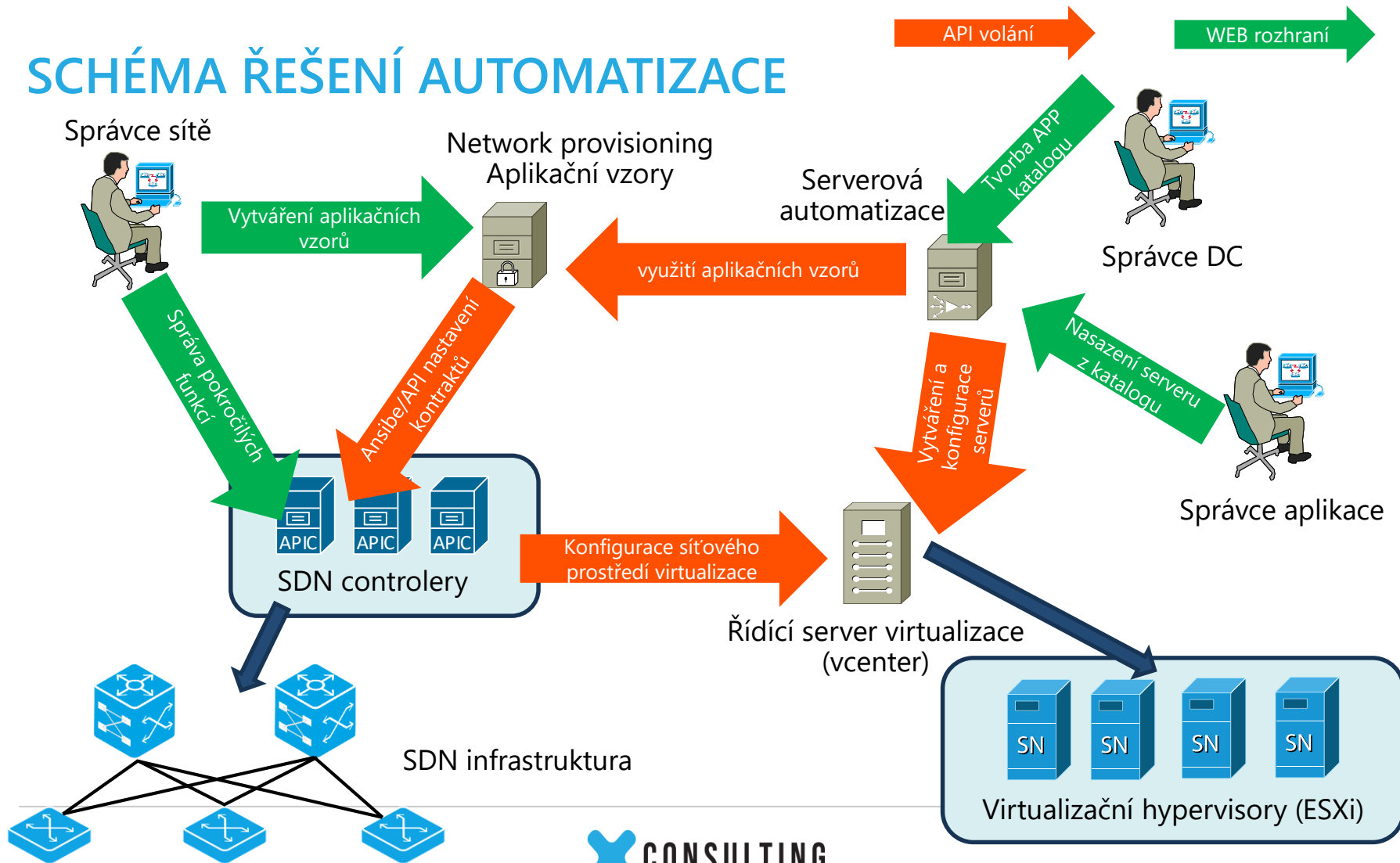
# AUTOMATIZACE FILTRAČNÍCH PRAVIDEL V DC

## Co potřebujeme pro automatizaci

- **Definovat standardní pravidla** pro danou aplikaci
- Pomocí **API v SDN** infrastruktury 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](mailto:jaroslav.sedlacek@xconsulting.cz)

