Standardizace infrastruktury PČR v rámci projektu MKI II.

Sjednocení konfigurace napříč celou sítí, zjednodušení správy a významné zvýšení bezpečnosti a odolnosti provozu – a to vše bez větších odstávek provozu kritické instituce a jejího fungování.

E-government 2026, Mikulov

collapo
lepší spolupráce

Ing. Jan Holub

ALEF

8.9.2026

Jak vznikala původní síť

Heterogenní prostředí infrastruktury

Každá lokalita nesla otisk doby/projektu, kdy vznikla. Různé stáří HW, odlišný design a konfigurace.

Legislativa a compliance

ZoKB, NIS2 — segmentace, auditní stopa, šifrování komunikace, …

Komplexita správy

Nejasně oddělené kompetence, specifické podmínky každé lokality, lokální změny bez vztahu ke globálnímu standardu.

Omezené zdroje

Různá úroveň znalostí napříč kraji a koncepce správy sítě.
Nemožnost zastupitelnosti mezi kraji/PP s ohledem na různorodost prostředí.
Dílčí projekty s ohledem na dostupné finanční prostředky.

Vysoké nároky na dostupnost

Krizové řízení, IZS — výpadek infrastruktury má reálný dopad na výkon veřejné moci.

Bezpečnost

Politiky a hardening se liší kraj od kraje a je ovlivněn i limitacemi technologií samotných.

Motivace pro změnu

IT Provoz

- Reaktivní provoz — hasí se incidenty místo prevence
- Know-how vázané na jednotlivce
- Každá změna = ruční práce na stovkách zařízení

Vedení

- Právní a reputační riziko (nesoulad s ZoKB, NIS2)
- Nelze slíbit termín řešení incidentu
- Bezpečnostní riziko

Ekonomická

- Skryté náklady — hodiny troubleshootingu místo rozvoje
- Neplánované výdaje při výpadku end-of-life hardware
- Špatná predikovatelnost nákladů do budoucích let

Cíle standardizace

Složitost správy a nezastupitelnost	→	Jednotné šablony a politiky napříč sítí
Heterogenní prostředí a EOL hardware	→	Sjednocená baseline a řízený lifecycle zařízení
Nejednotné, sdílené admin přístupy	→	Centralizovaná AAA — Cisco ISE / TACACS+
Chybějící viditelnost provozu	→	Full NetFlow na nové HW platformě
Těžko splnitelná NIS2 / ZoKB	→	Centrální vynutitelnost standardů a auditovatelnost politik
Omezené zdroje — lidé i rozpočet	→	Automatizace onboardingu, hromadných změn a údržby

Standardizace jako princip

Stejný princip platí na každé vrstvě sítě — liší se jen nástroj. Standardizace vychází z koncepce MV ČR.

WAN

Cisco SD-WAN

LAN

Cisco Catalyst Center

Identita a přístup

Cisco ISE / TACACS+

Viditelnost

Full NetFlow + Analytics

Automatizace a governance

Centrální management, šablony, standardy a řízení změn

Realizace programu MKI II. pro Policii ČR

Standardizace L3, WAN (SD-WAN) a Access vrstev

collapo

Kontext MKI II.

1. Společný technologický standard vycházející z koncepce MV ČR
2. Oddělení rolí poskytovatel transportní sítě (MV) x zákazník (PČR)
3. Vazba na projekty ISIK, MKI I.
4. Měnící se potřeby v průběhu programu

Oblasti standardizace

1 Typ lokality

Rozdělení lokalit dle významu na velké uzlové objekty, střední uzlové objekty a malé koncové objekty.

2 Design lokalit dle typu

Standard zařízení, jejich zapojení a konfigurace.

3 Centrální politika

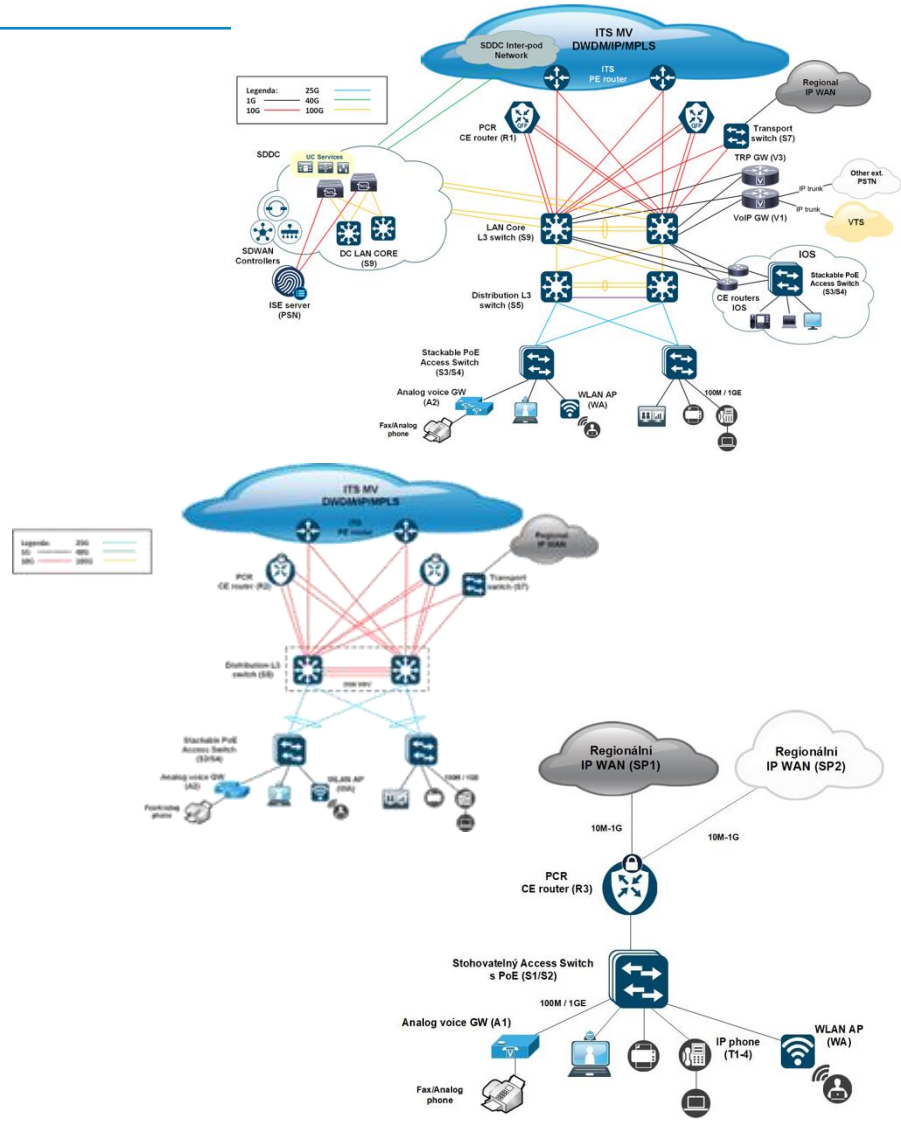
Jednotné názvosloví, systém hostnames, IP plán, nová management síť, centrální systémy (NTP, DNS, AD pro management, ISE/TACACS+, logování, flow data).

4 Konfigurační templaty

Aplikováno pro WAN i LAN. Využití standardních templatů dle typu a topologie lokality pro WAN i LAN část.

5 Bezpečnostní baseline

Jednotná bezpečnostní baseline vynucována centrálním management WAN i LAN.



collapo

Proč SD-WAN namísto tradičních WAN sítí

Dlouhý lead-time nové lokality

Zřízení nové MPLS/KIVS přípojky na pobočku trvá týdny až měsíce — brzdí rozšiřování sítě.

Drahý transport

KIVS L2 okruhy jsou dražší než L3 VPN/internet za srovnatelnou šířku pásma.

Chybí viditelnost

Provoz a incidenty na desítkách/stovkách lokalit se řeší reaktivně, bez centrálního přehledu.

Ruční CLI konfigurace

Stovky routerů konfigurovaných box-by-box → chybovost, nekonzistence, pomalé změny.

Roztříštěná bezpečnost

Politiky, ACL a segmentace se liší lokalitu od lokality — těžko auditovatelné.

Tlak legislativy

NIS2 a ZoKB vyžadují prokazatelnou segmentaci, řízení přístupu a incident response napříč celou sítí.

CE Routery – SD-WAN

Software-defined WAN odděluje řídící a datovou část sítě. Místo ručně konfigurovaných routerů přes CLI vzniká centrálně řízená overlay síť nad libovolným transportem (MPLS, internet, LTE/5G, satelit).

Klíčové principy a benefity

- Politika a konfigurace se řídí centrálně, ne per-zařízení
- Šifrovaný IPsec overlay mezi všemi lokalitami „by default“ a bez možnosti vypnutí
- Multi-transport aktivní/aktivní připojení (MPLS/L2 KIVS/Internet - 5G/LTE/ADSL)
- Automatizované nasazení – Zero-touch nasazení
- Templaty per typ a design lokality

Komponenty SD-WAN řešení

WAN Edge

Fyzický router na lokalitě, nese provoz

SD-WAN Manager

Centrální GUI, konfigurace, monitoring, orchestrace

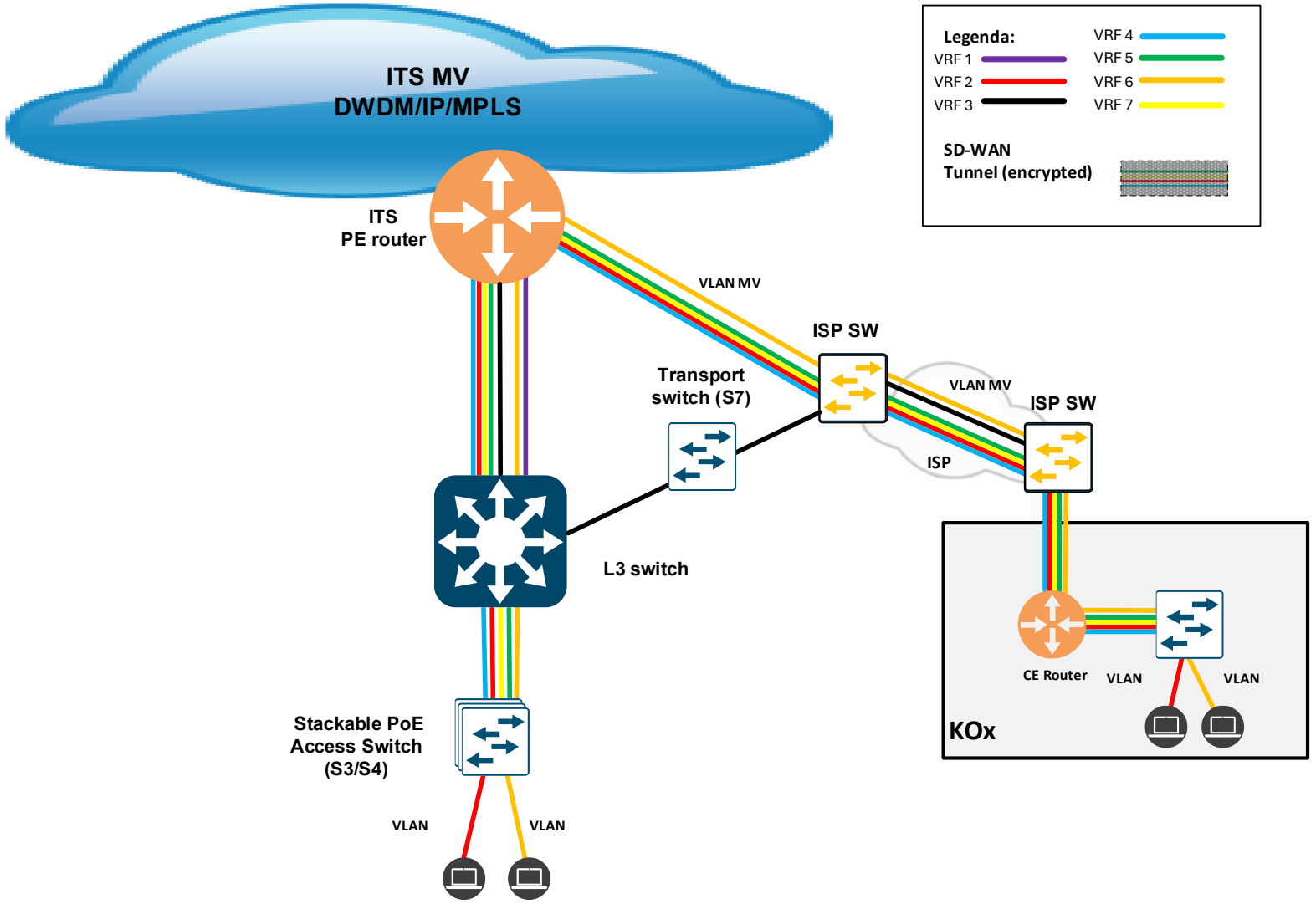
SD-WAN Controller

Distribuce routovacích a bezpečnostních politik (OMP)

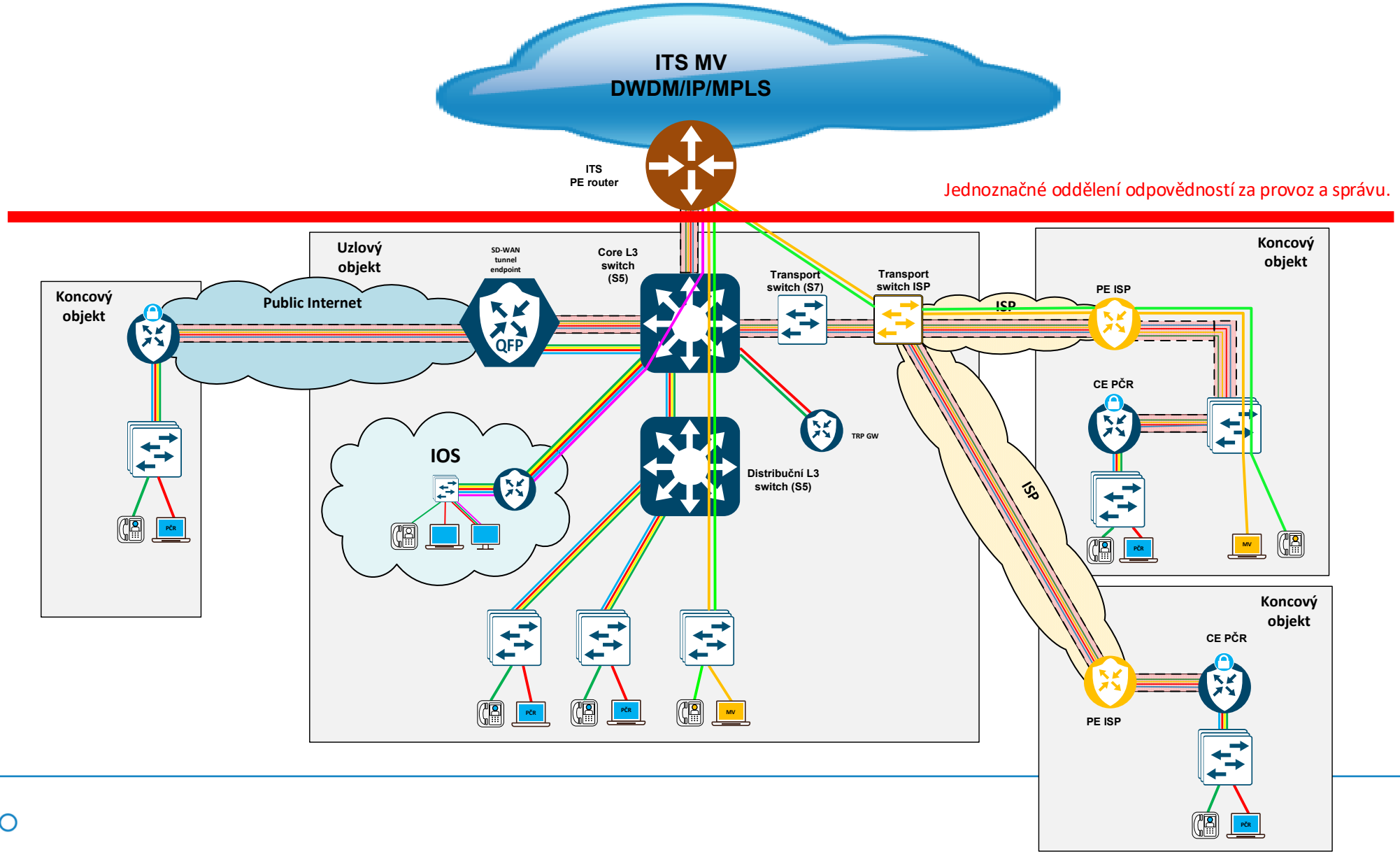
SD-WAN Validator

Autentizace a orchestrace prvotního připojení zařízení

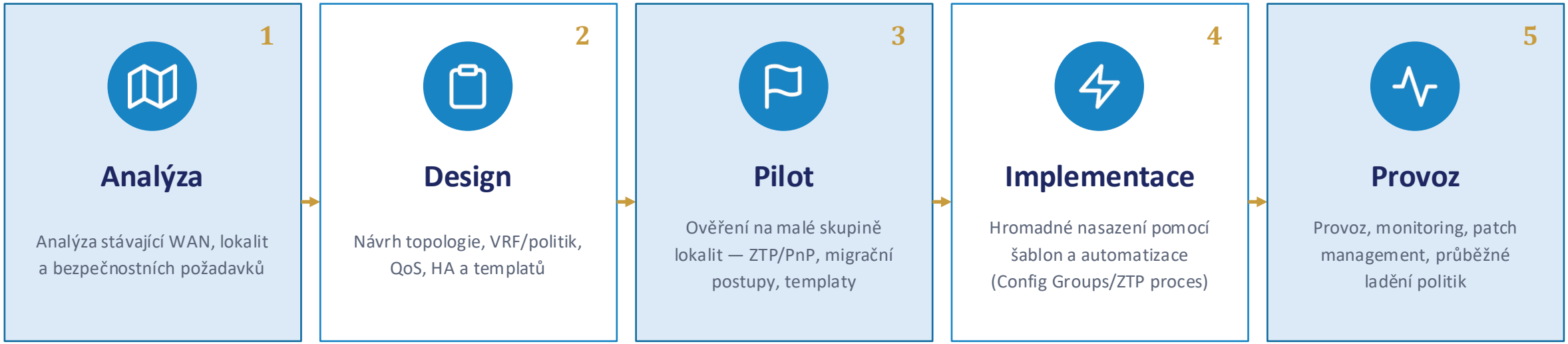
Komunikace na lokalitě před nasazení SD-WAN



Komunikace na lokalitě po nasazení SD-WAN



Zkušenosti z projektu aneb proč se toho nebát a na co nezapomenout



- Důkladná analýza stávající WAN a jednotlivých lokalit
- Sběr požadavků na nové funkcionality a budoucí plánovaný rozvoj
- Ověření požadavků ZoKB, NIS2 a jejich zakomponování do designu
- Ověření segmentace na úrovni samostatných L3 sítí (VRFs) a případné změny do designu
- Proškolení budoucích administrátorů
- Standard jednotlivých typů lokalit

- Ověření připravenost centrální infrastruktury
- Standardizace infrastruktury před nasazením SD-WAN
- Pilotní nasazení a odladění konfiguračních templatů na relevantním vzorku lokalit
- Informovanost v průběhu celého projektu všech zúčastněných stran
- Minimalizace dopadu na jednotlivé lokality
- „Freeze“ periody na úpravy v síti

Benefity SD-WAN řešení pro veřejný sektor

Centrální řízení a viditelnost

Jedno rozhraní (SD-WAN Manager) pro konfiguraci, monitoring a troubleshooting stovek lokalit.

Automatizované nasazení

Zero-Touch/Plug-and-Play provisioning — nová lokalita naběhne bez zásahu lokálního IT.

Šifrování „by default“

IPsec overlay mezi všemi WAN Edge routery automaticky, bez ruční konfigurace VPN tunelů a **nemožnost vypnutí šifrování.**

Segmentace politik a VRF

Oddělení provozu podle citlivosti a agendy — základ pro splnění NIS2/ZoKB požadavků.

Vynucení templatů konfigurace

Jednotlivé lokality jsou implementovány dle připravených standardů centrálním správcem.

Nákladová efektivita

Kombinace levnějších transportů (L3 VPN, LTE/5G) s MPLS snižuje náklady na přenos dat.

Odolnost a kontinuita

Multi-transport, aktivní/aktivní připojení, rychlý failover — méně výpadků kritických služeb. Možná záloha přes internet k privátním okruhům.

Rychlejší změny

Změna politiky pro celou síť během minut místo postupné konfigurace box-by-box.

Cisco Catalyst Center

Místo ručně konfigurovaných switchů přes CLI na každé lokalitě vzniká centrálně řízená přístupové (access) síť.

Princip

- Fabric-based přístupová síť řízená centrálně
- Jednotné šablony pro switche (baseline konfigurace)
- L3 Core a Distribuční switche navrhované společně s WAN i Access vrstvou

Automatizované onboardování

Nový switch se zapojí a nakonfiguruje podle šablony bez ruční práce

Segmentace na L2/L3

Konzistentní VLANy a politika napříč všemi lokalitami

Assurance a telemetrie

Průběžné sledování stavu sítě a rychlá diagnostika

Konzistentní bezpečnostní baseline

Stejný hardening všude, bez výjimek podle historie lokality

Výstupy programu MKI II.

Centralizace a automatizace nahrazují ruční box-by-box správu stovek lokalit jak WAN tak LAN prostředí	**Konfigurace pro použití nového syslog serveru nasazena během jediného dne.**
Segmentace a šifrování „by default“ bez možnosti vypnutí	**Soulad se ZoKB a NIS2**
Nový HW zajišťující vyšší dostupnost, bezpečnost a umožňující budoucí rozvoj	**Nahrazen HW starý i více než 15 let a po ukončení podpory ze strany výrobce.**
Úspěch projektu stojí nejen na přípravě: analýza, standardy, automatizace a bezpečnost od začátku, ale i na vůli dodržet nastavené standardy	**Během projektu bylo občas složité upřednostnit standard před pohodlností výjimky.**
Standardizace umožňuje spolupráci při provozu a podpoře sítě	**Umožnilo mezikrajovou spolupráci při incidentech a konzultace konfiguračních změn.**
Standardizace velkých lokalit umožnila bezodstávkové provádění změn a upgradů zařízení	**Bylo možné provést upgrade prvků na LVH během plného letního provozu.**
Centrální správa umožňuje rychlou reakci na bezpečnostní hrozby	**Upgrade SW zařízení z důvodu zranitelnosti na tisících zařízeních PČR během jediného týdne.**

collapo

lepší spolupráce

ALEF

Děkuji za pozornost

sales@collapo.com

+420 605 232 026