Architektura SecureX

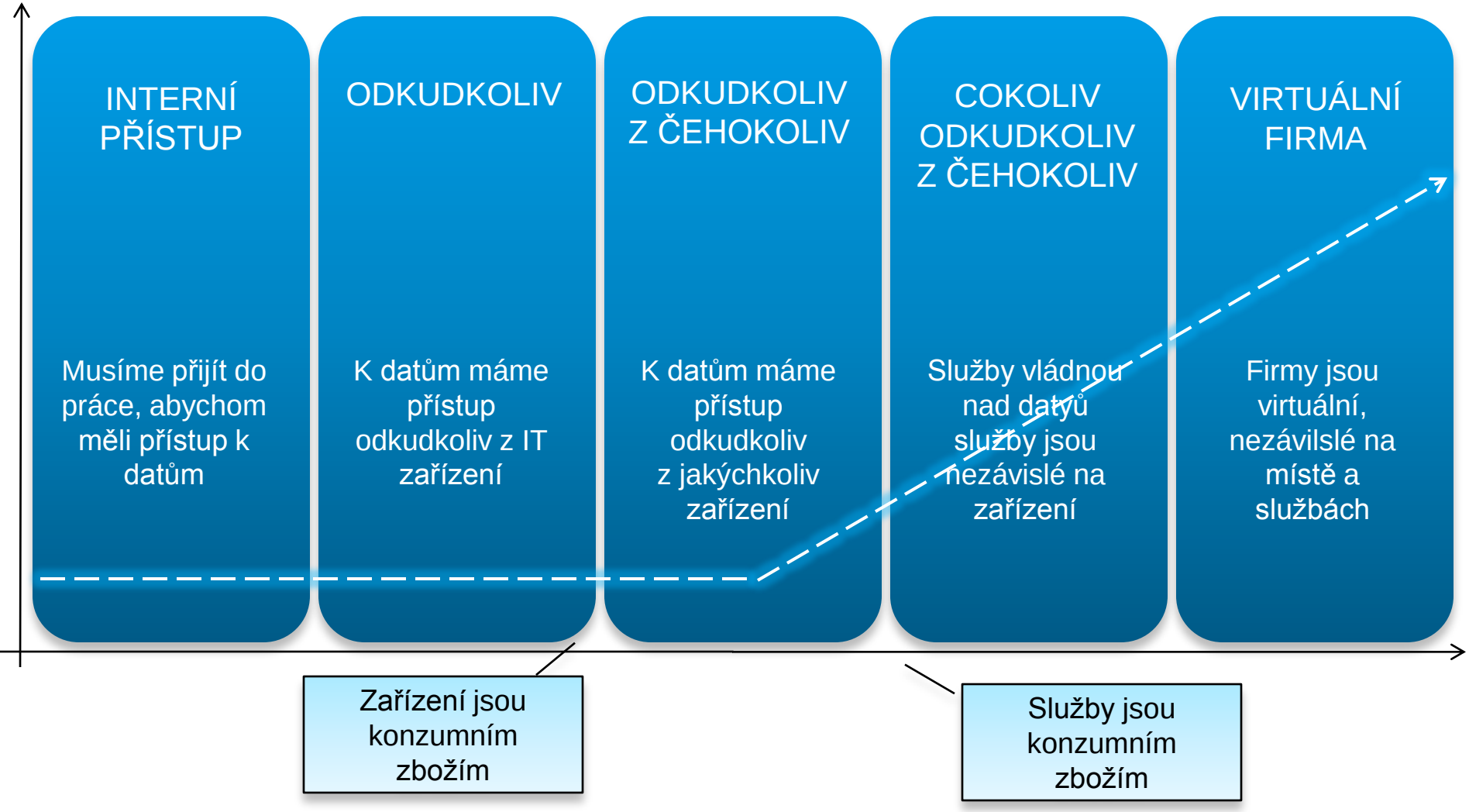
Ivo Němeček, CCIE #4108
Manager, Systems Engineering

25.4.2012, Cisco Expo Praha

Program

- IT se mění a má to dopad na bezpečnost
- SecureX architektura
- Bezpečný přístup a mobilita
- Bezpečná síť a hranice sítě
- Zabezpečené datové centrum

IT prostředí se mění…

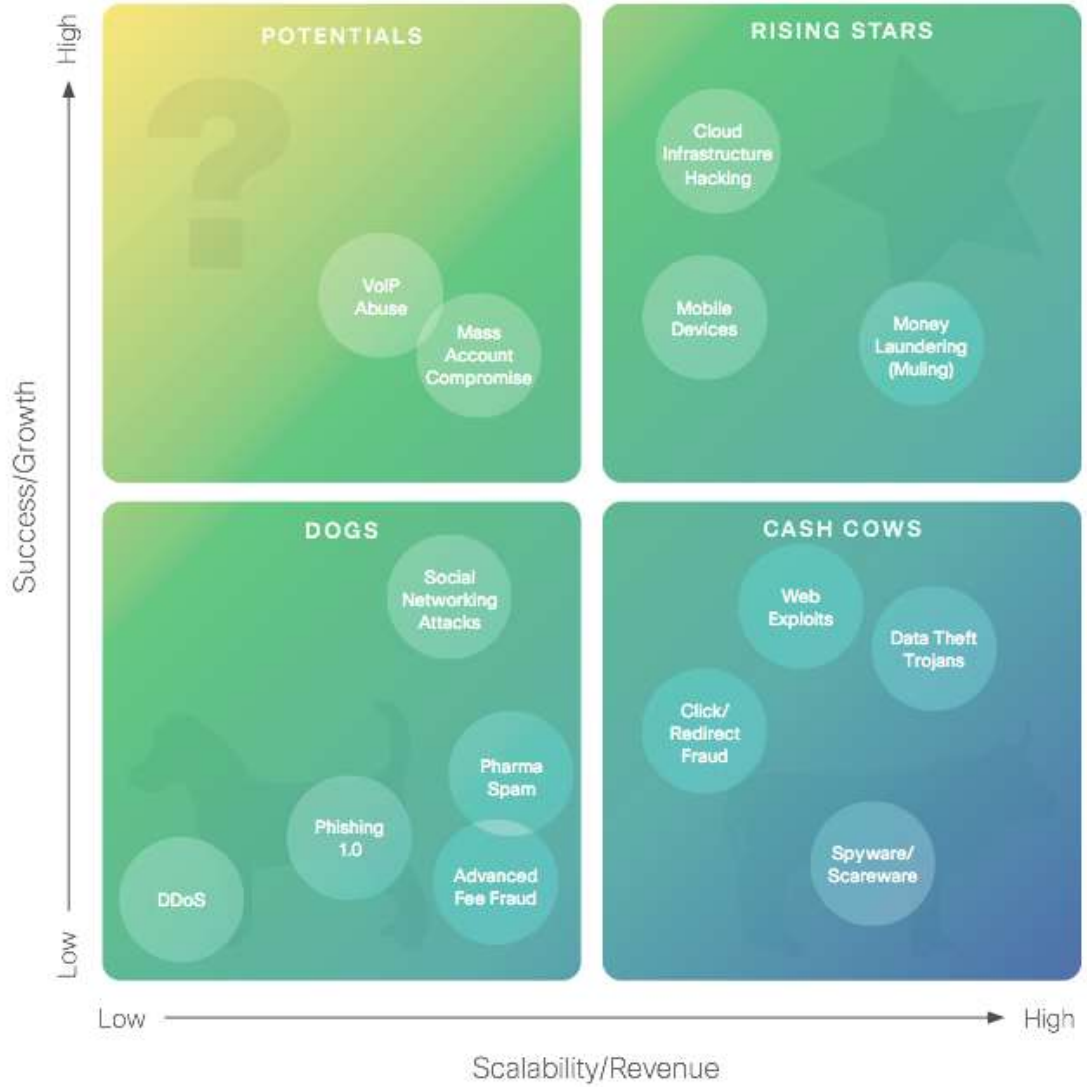


… a bude se měnit
(časová linka vymírání různých druhů)

- 2012: faxy
- 2014: bloudění
- 2017: pevný ethernet pro koncové uživatele
- 2018: laptop (nahradí ho tenký klient)
- 2020: © copyright
- 2021: oznamovací tón telefonních hovorů - - - - - - -
- 2027: telefonní čísla +420 2 2143 5111
- 2030: klíče
- 2033: mince
- 2045: zaměstnání (“oblak lidí” – mturk.com)
- 2049: papírové noviny
- 2050: kancelářské budovy

Zdroj: http://rossdawsonblog.com/weblog/archives/2007/10/extinction_time. a Cisco Innovation workshop, December 2010

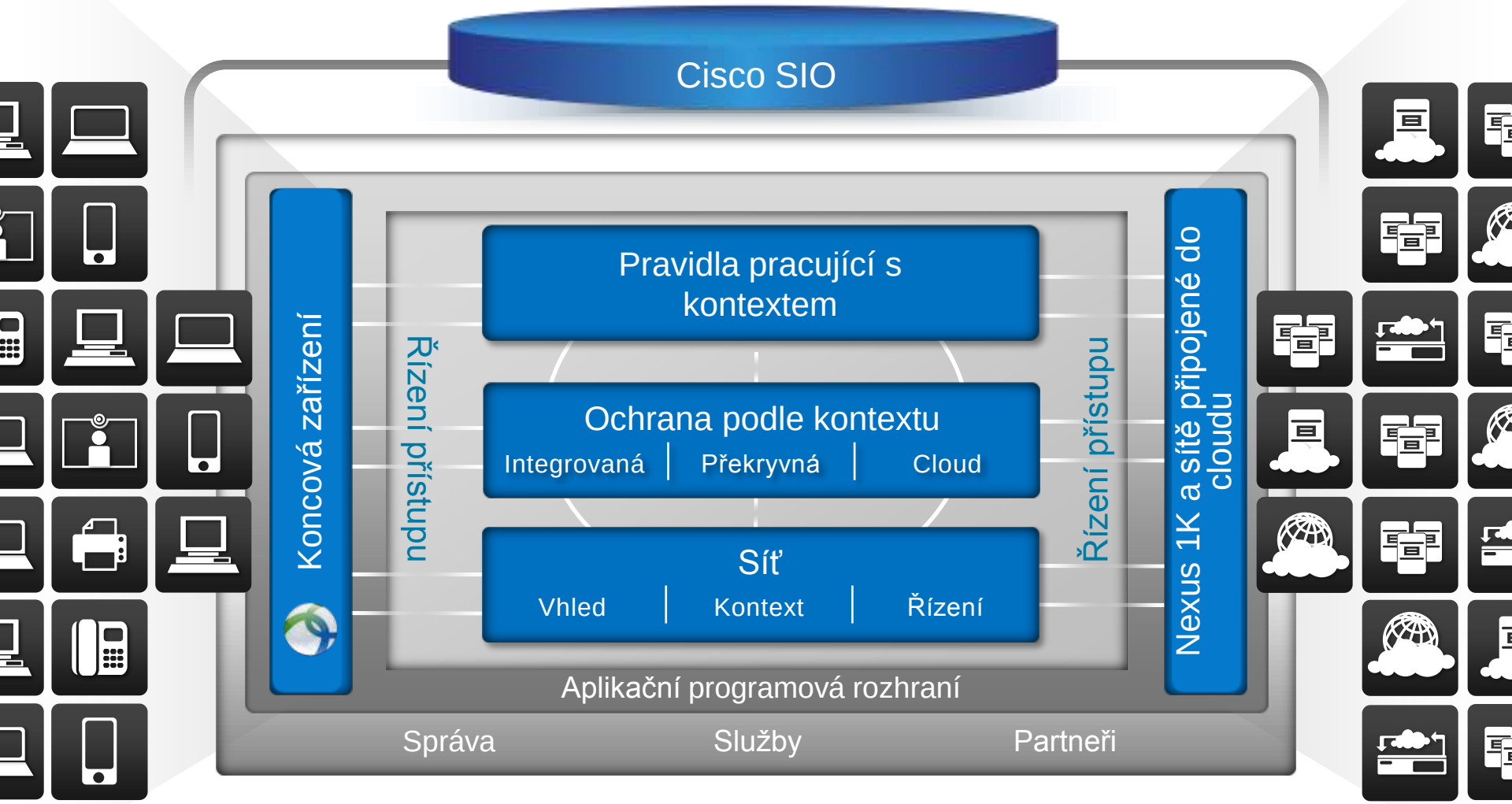
I hrozby se proměňují
(Cisco Annual Security Report)



Podívejme se, jak chránit …

- všechna možná zařízení, ať jsou kdekoliv
- Široké spektrum aplikací
- data směřující do cloudu
- virtualizovaná datová centra
- A to vše proti stále komplexnějším hrozbám

Architektura Cisco SecureX



Security Intelligence Operations (SIO)

Cisco SecureX řešení

Dynamické prostředí podnikových sítí

Bezpečný přístup a jednotná pravidla

Rozlišení zařízení, uživatelů a rolí

ISE, VPN, ASA, MACSec, Síť, AnyConnect

Vzdálený přístup

Bezpečná mobilita

Rozšíření firemní sítě

ISE, MACSec, ScanSafe, VPN, AnyConnect, WSA

Útoky, malware

Síť a hranice sítě

Ochrana přenášených dat

ISE, Router, VPN, ASA, IPS, ESA

Virtualizace

Bezpečná datová centra a cloud

Ochrana mozku firmy

VPN, ASA, Nexus 1000V, VSG

Cisco SecureX

V kontextu je síla

Bezpečný přístup

ÚLOHA

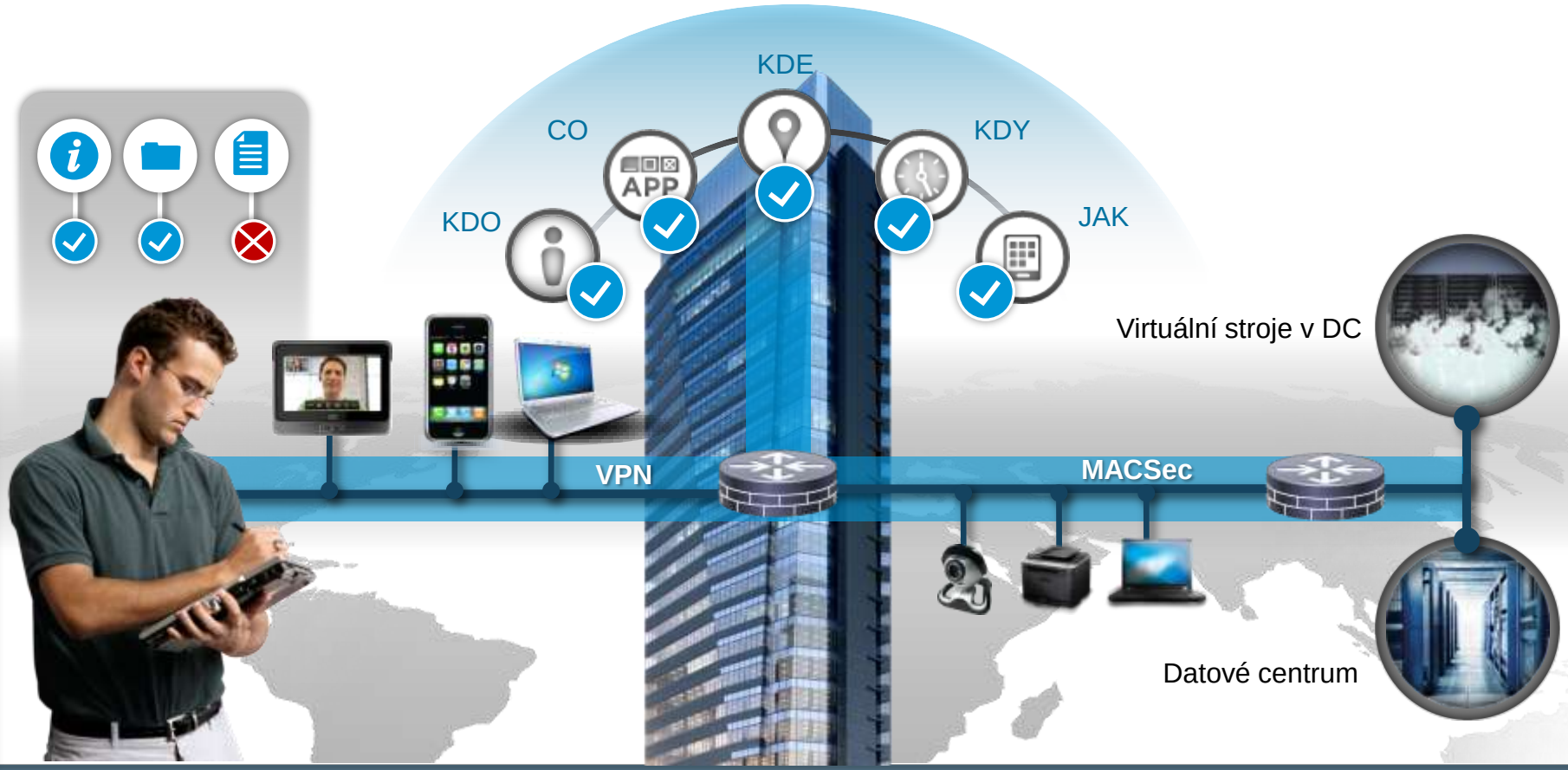
Přístup podle zařízení, totožnosti a role

Přístup pro hosty

Prosazení pravidel od koncového zařízení až po datové centrum

Zajištění důvěrnosti v celé síti

Řešení: TrustSec



CISCO ŘEŠENÍ

Konzistentni pravidla pracující s identitou - od libovolných zařízení po datová centra

Distribuce pravidel a informací do sítě

Bezpečností značky (Security Group Tagging) pro pružné prosazení kontextových pravidel

Součásti řešení TrustSec

Správa pravidel
Distribuce pravidel

Identity Services Engine (ISE)
Identity Access Policy System

Prosazování pravidel v síti

Cat 2900/3560/3700/4500/6500, Nexus 5000/7000
přepínače, bezdrátová a směrovaná infrastruktura

Cisco ASA, ISR, ASR 1000

Prosazování pravidel v koncových zařízeních

NAC Agent

Web Agent

Trvalý i dočasný klient pro prohlídku a léčbu

802.1x Supplicant
AnyConnect
OS-Embedded Supplicant

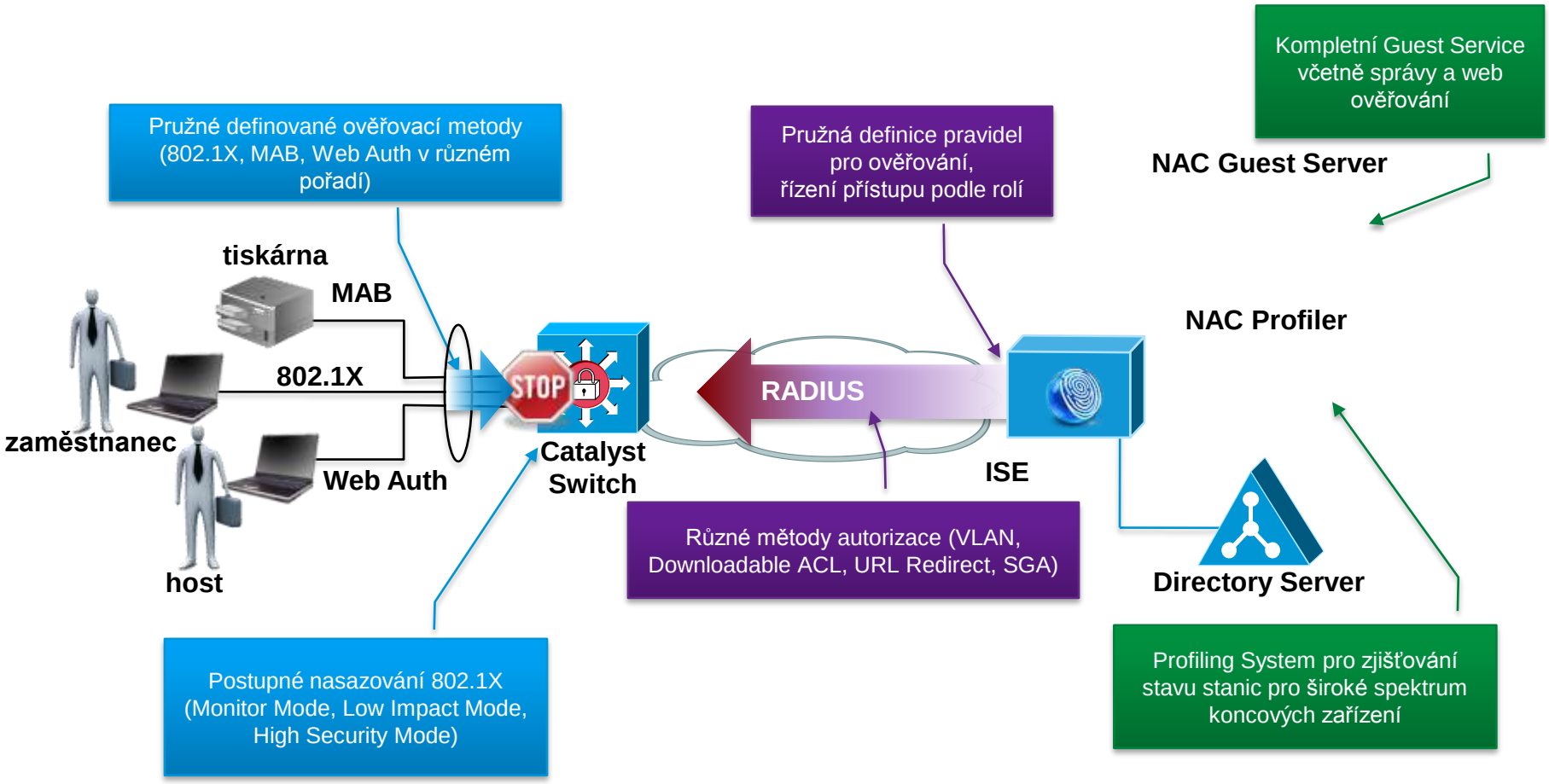

Dr. Sova
LAN
Známá WiFi
Dr. Blair
Today
Clear Window
Is Mr. Allen's lab work ready yet?
Not yet but i will let you know the moment it arrives
ZABEZPEČENÍ:
AnyConnect
ASA
ISE


Veřejné
WiFi
ZABEZPEČENÍ:
AnyConnect
ASA
ISE
VPN
ScanSafe

ZABEZPEČENÍ:

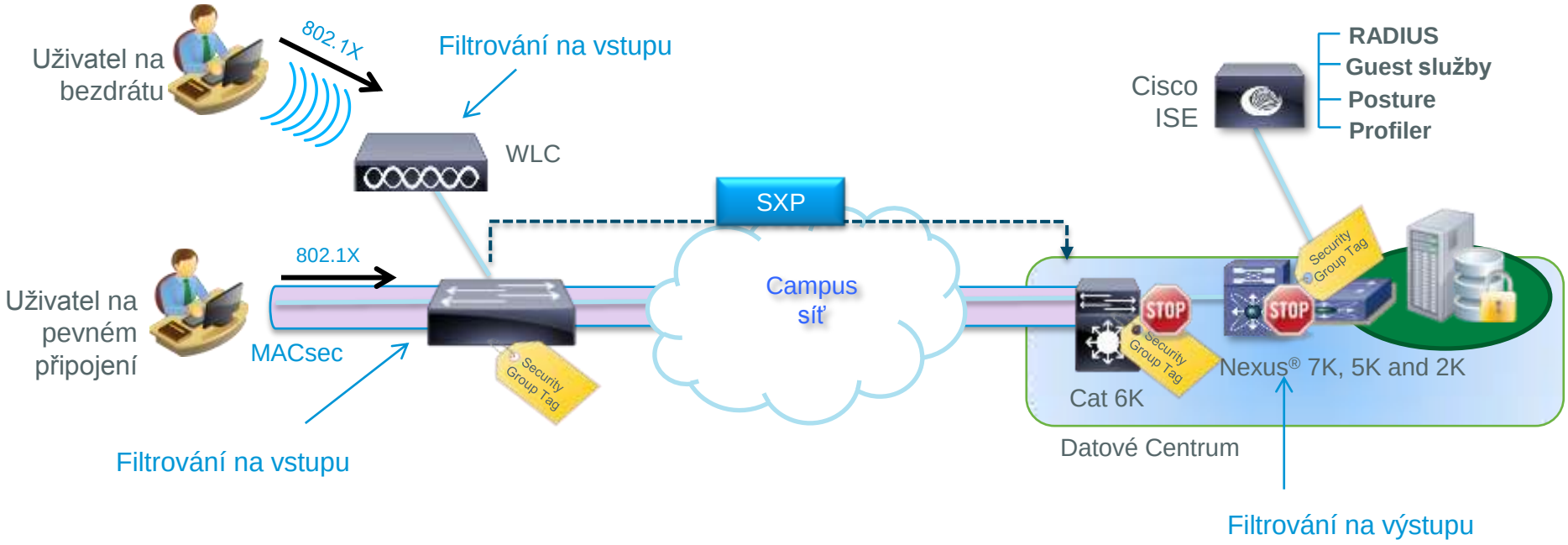
AnyConnect | ASA | ISE | VPN | ScanSafe

Trustsec řešení

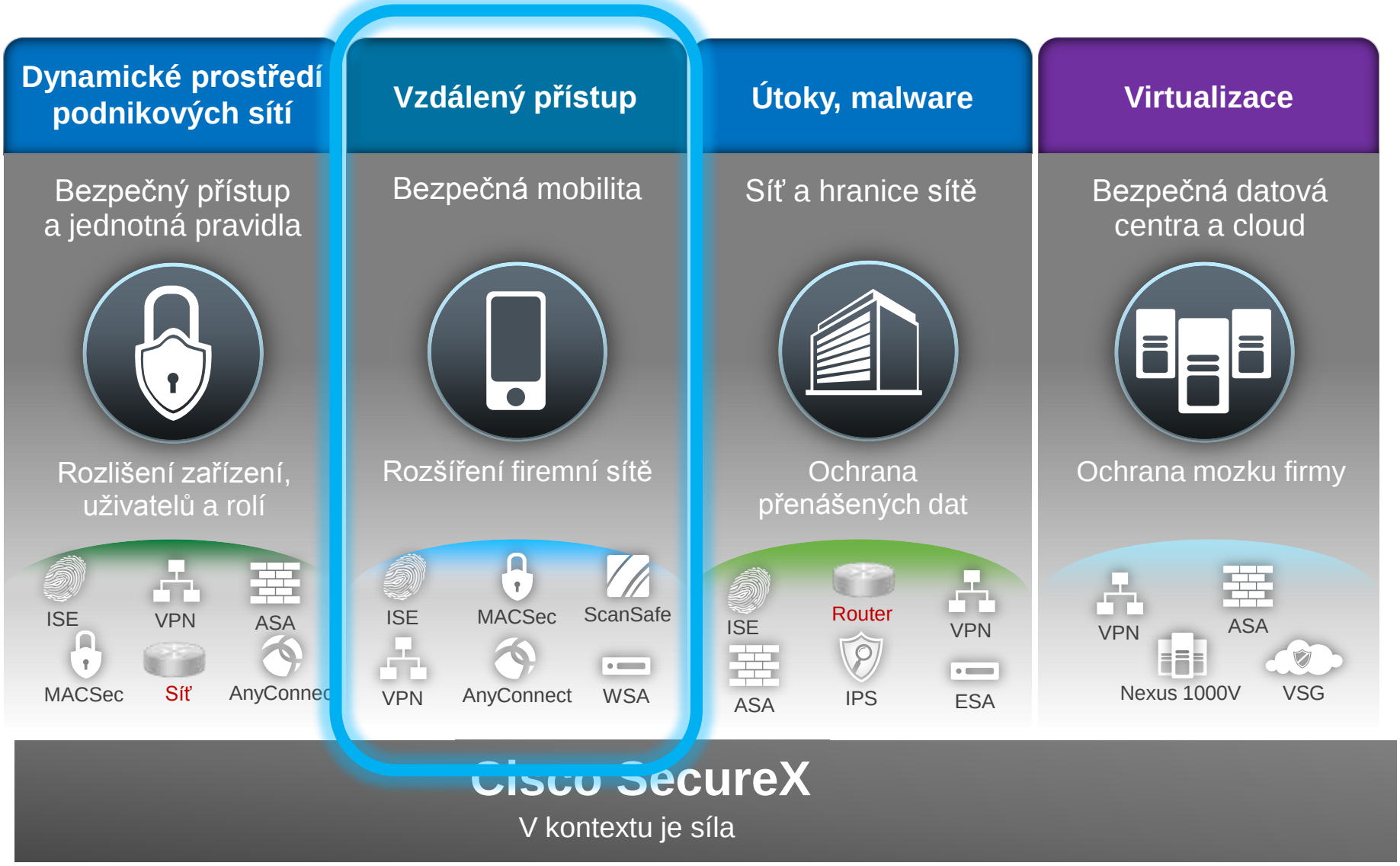


TrustSec vlastnosti

Šifrování, SGA, SXP



Cisco SecureX řešení



Bezpečná mobilita

ÚLOHA

Vysoce mobilní uživatelé potřebují přístup do sítě a ke cloud službám

Široké spektrum mobilních zařízení uživatelů ztěžuje definici pravidel

Ztráta zařízení zvyšuje riziko ztráty dat a porušování norem

Řešení

Libovolný uživatel s libovolným zařízením

Cisco AnyConnect

Access přepínače

ISR

ASA

TrustSec

WSA

ScanSafe

Interní, cloud & sociální aplikace

ORACLE

Microsoft SharePoint

Cisco webex

amazon web services

Salesforce

CISCO ŘEŠENÍ

Bezpečné připojení

Šifrování MACsec na celé trase

Hybridní bezpečnost webu

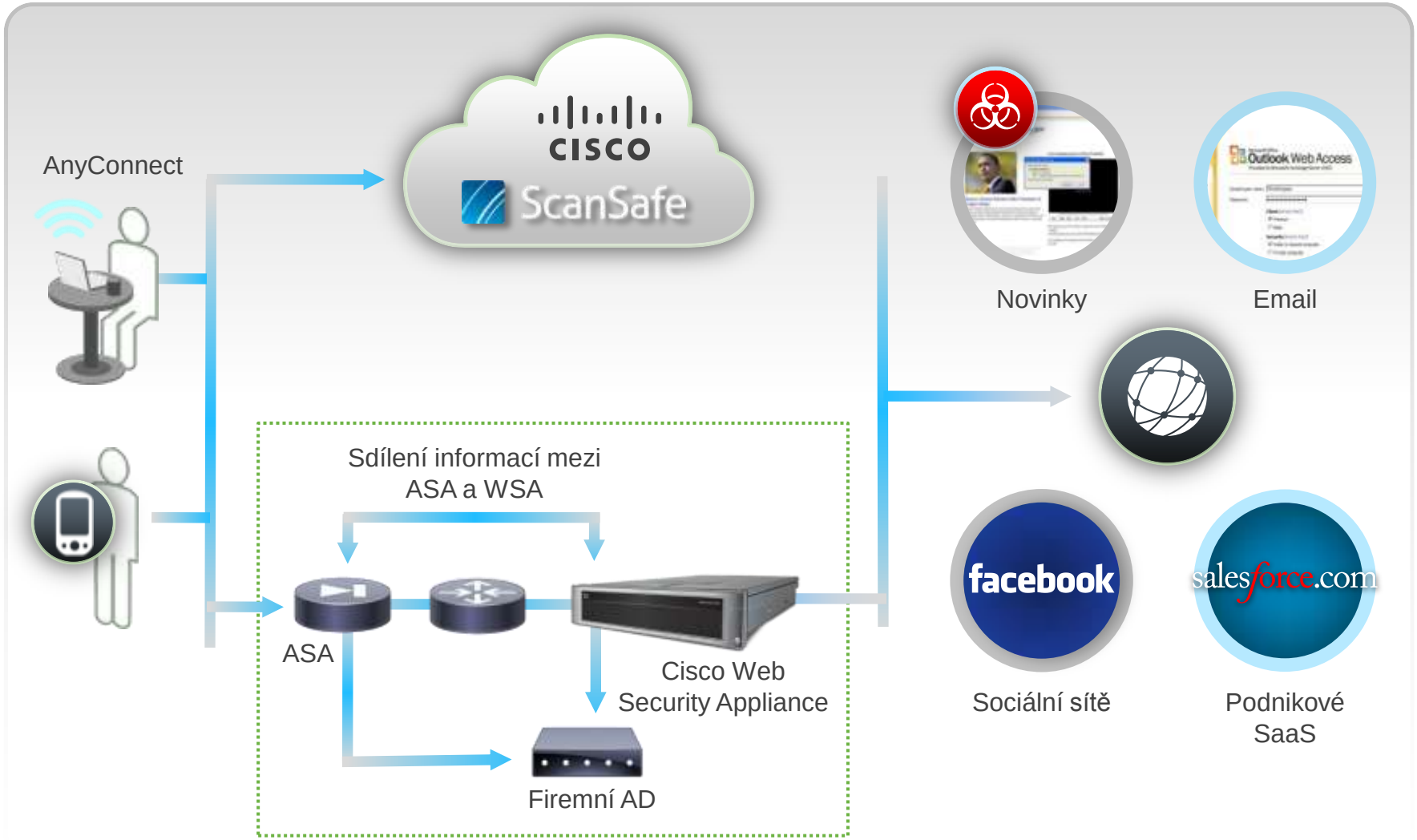
Široká podpora zařízení: Windows XP/7,MAC OSX, Linux, Apple iOS (iPhone & iPad), Nokia Symbian, Webos, Windows Mobile, Android*

Bohaté funkce nepřetržitá ochrana hybridní (cloud nebo místní) řešení

AnyConnect klient

- Přítulné rozhraní
- Funkce pro WLAN i LAN
- Integrovaná správa připojení
- Bohaté funkce
  - Neustálé připojení
    Spolupráce s WSA a ScanSafe
  - Integrovaná inspekce stanic
  - Podpora pro ScanSafe cloud security
  - Mnoho podporovaných zařízení a OS

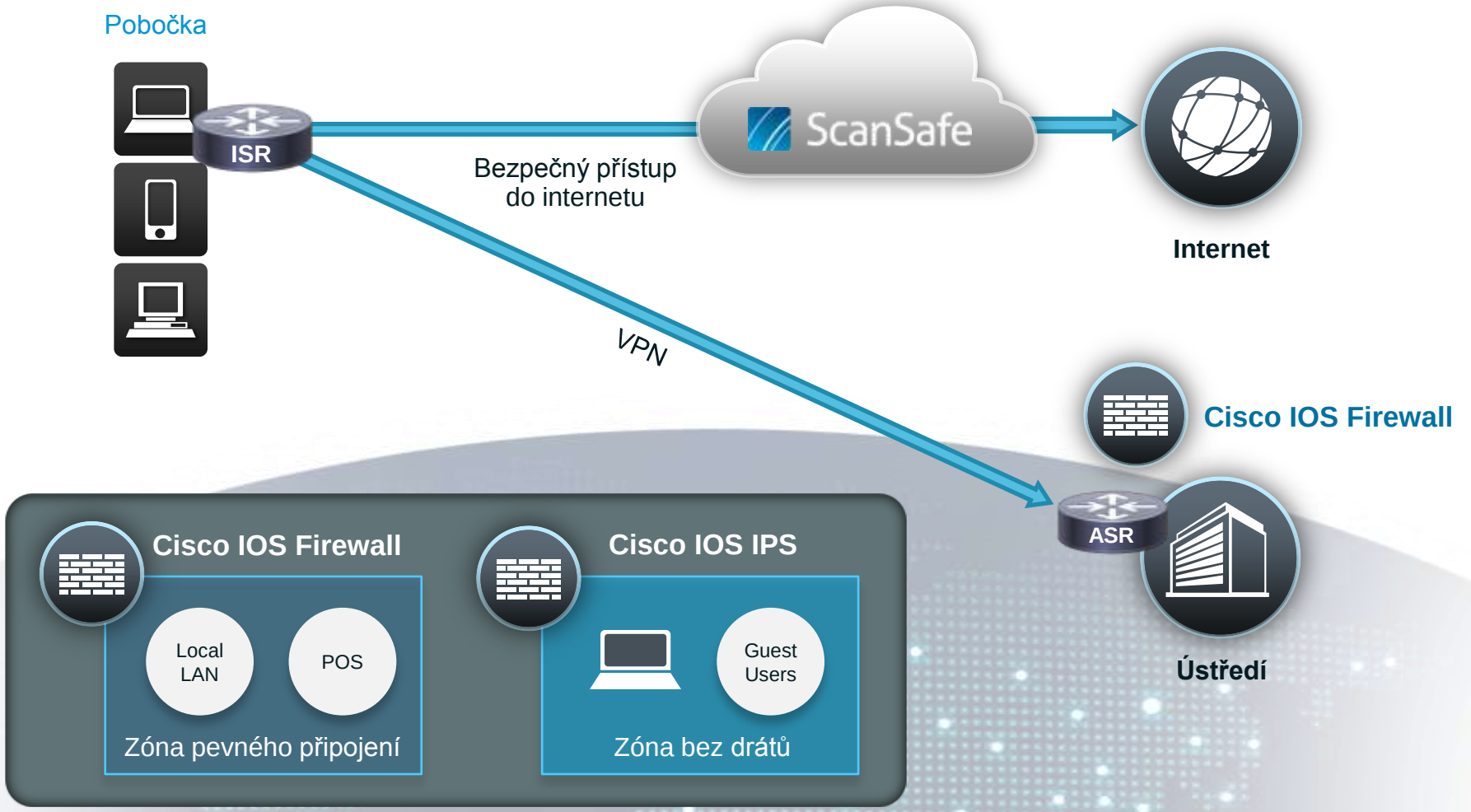
Hybridní ochrana web komunikace
s AnyConnect klientem




LAN
ZABEZPEČENÍ:
AnyConnect
MACSec
VPN
Web Security Appliance


3G
CHELSEA
FOOTBALL CLUB
ZABEZPEČENÍ:
AnyConnect
MACSec
VPN
Web Security Appliance
ScanSafe

Hybridní ochrana webu komunikace
s ISR směrovači




ISR
ZABEZPEČENÍ:
Firewall
IPS
VPN
ScanSafe
ISE


ZABEZPEČENÍ:
ASA
IPS
VPN
ScanSafe
ISE
AnyConnect

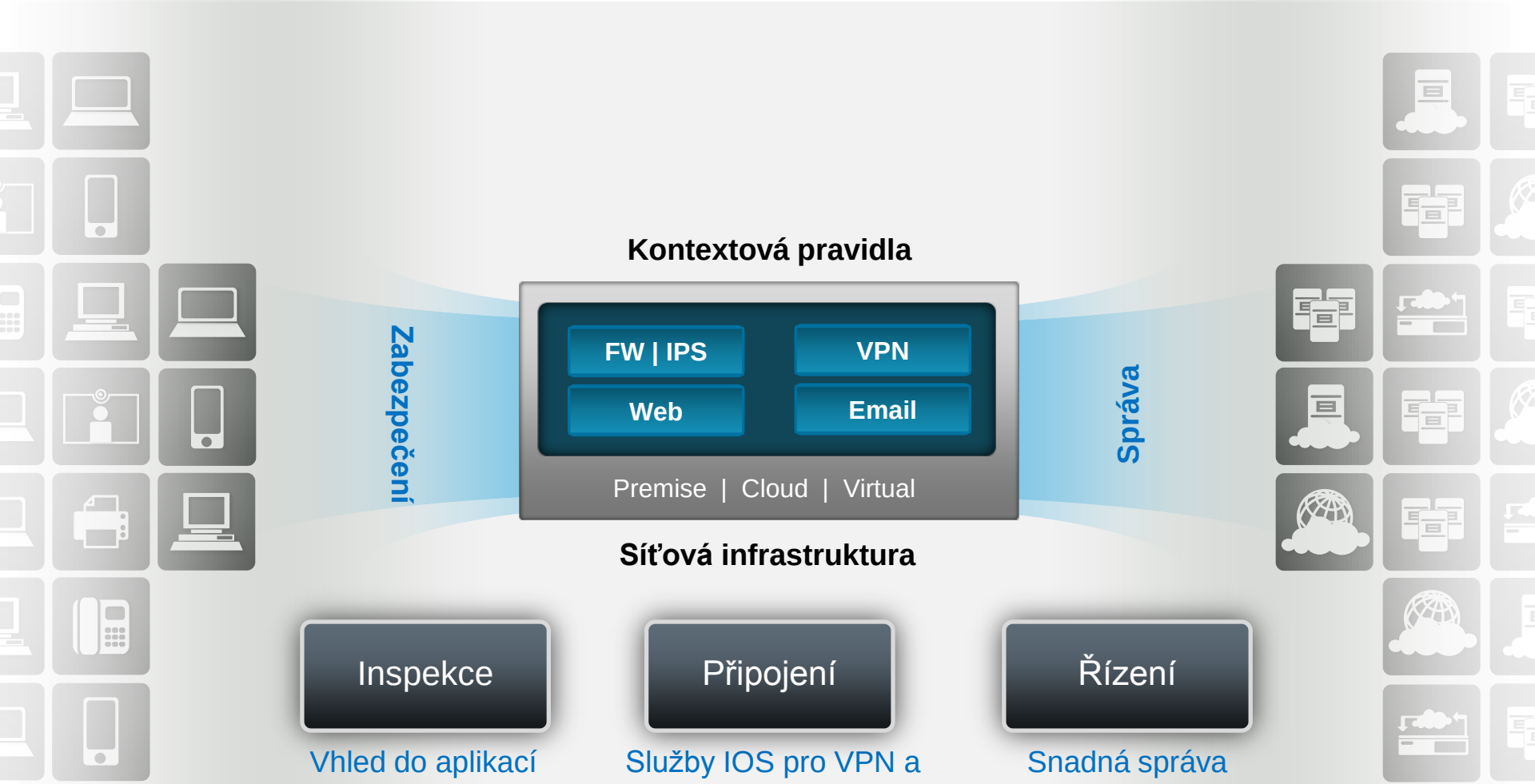

ISR
E1 SPOJ
ASA
IPS
VPN
ScanSafe
ISE
AnyConnect

Cisco SecureX řešení

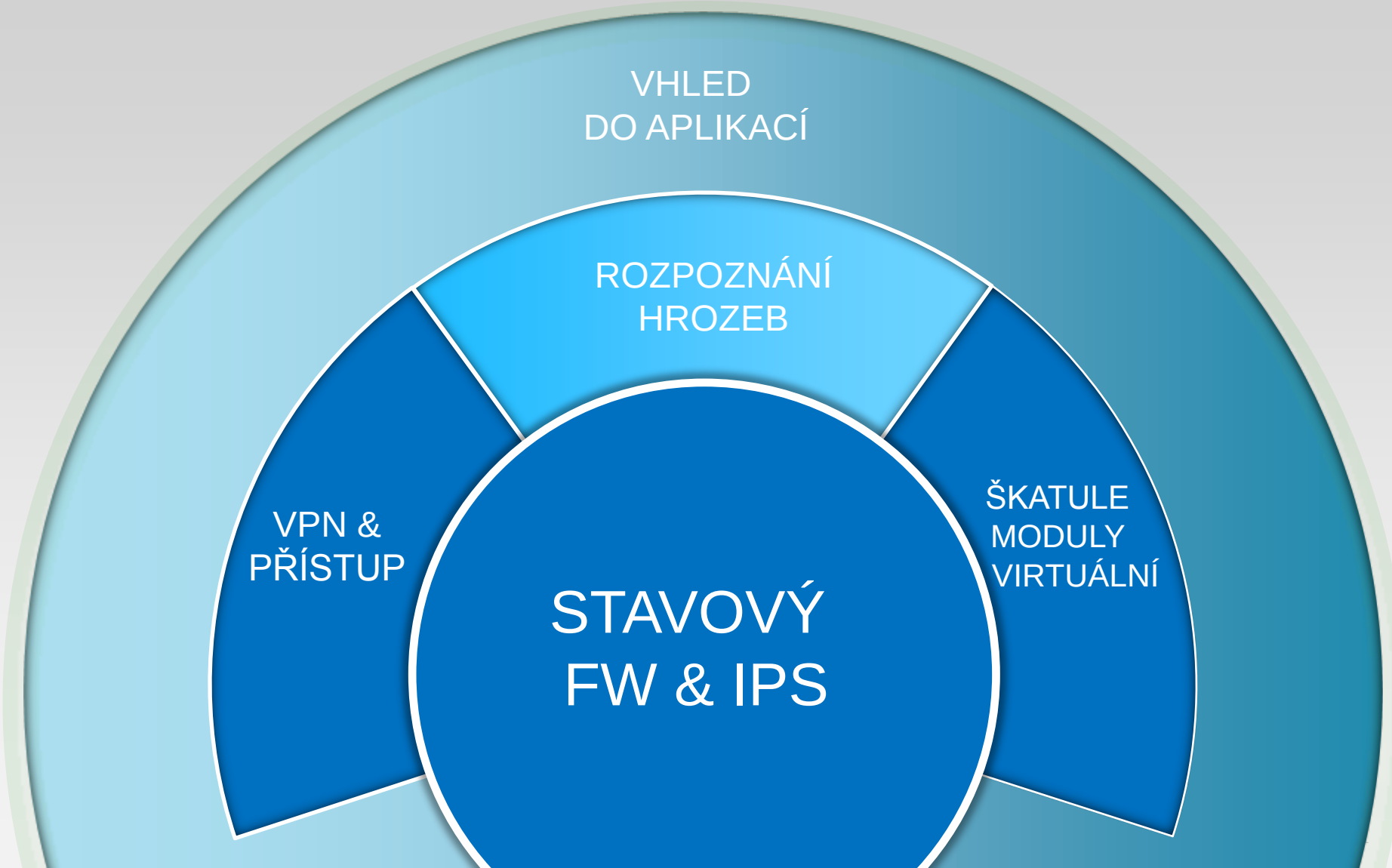
Cisco Securex

V kontextu je síla

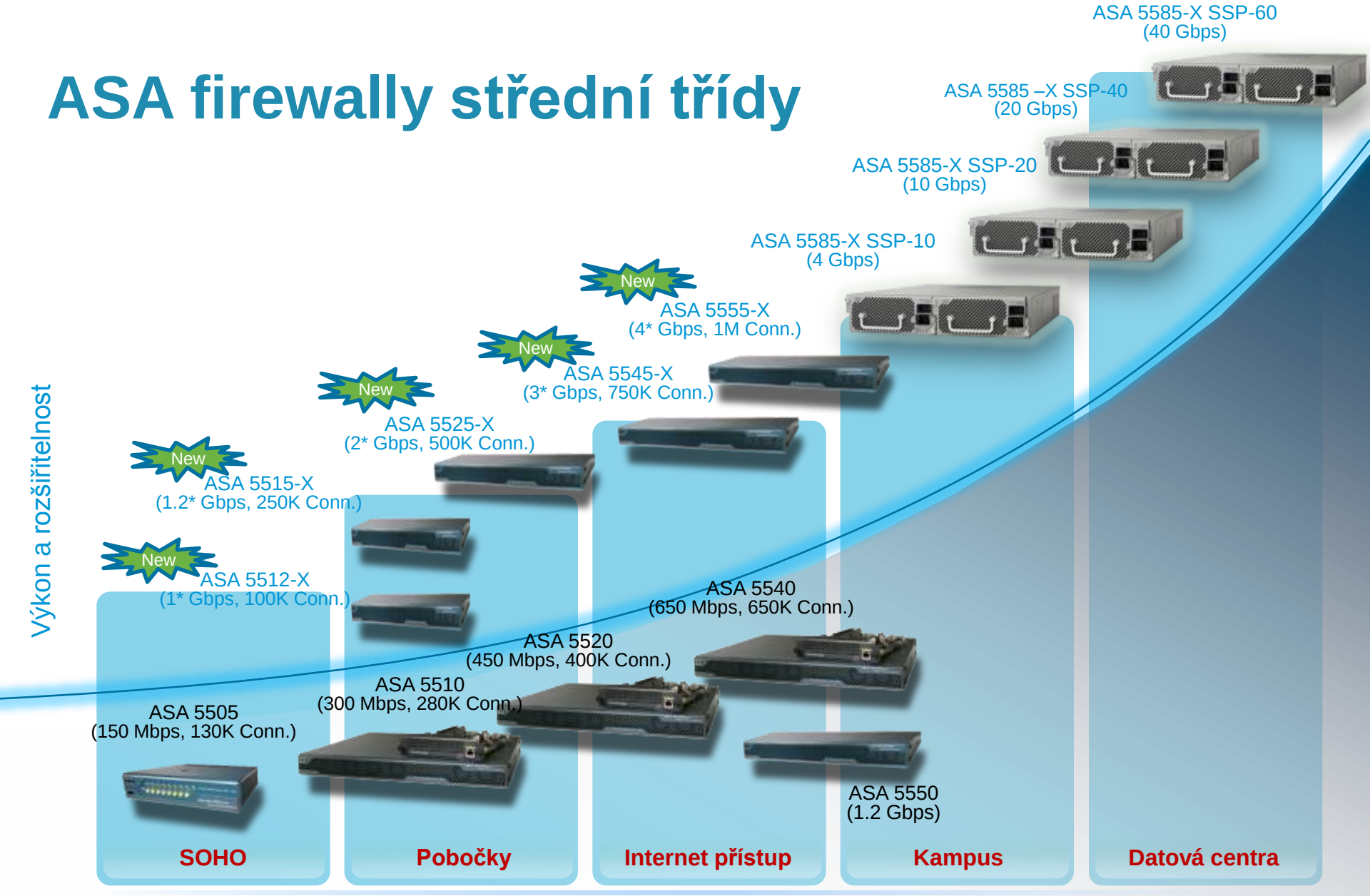
Řešení pro ochrany proti útokům



Kontextové a aplikační firewally



ASA firewally střední třídy



* Výkon bude upřesněn

Nová ASA CX

- Kontextový firewall
- Aktivní a pasivní ověřování
- Vhled do aplikací a jejich řízení
- Identifikace zařízení
- Reputační filtrování
- Místa připojení

ASA CX architektura

ASA 5585-X MultiScale™

Počet paralelních spojení
10 millionů

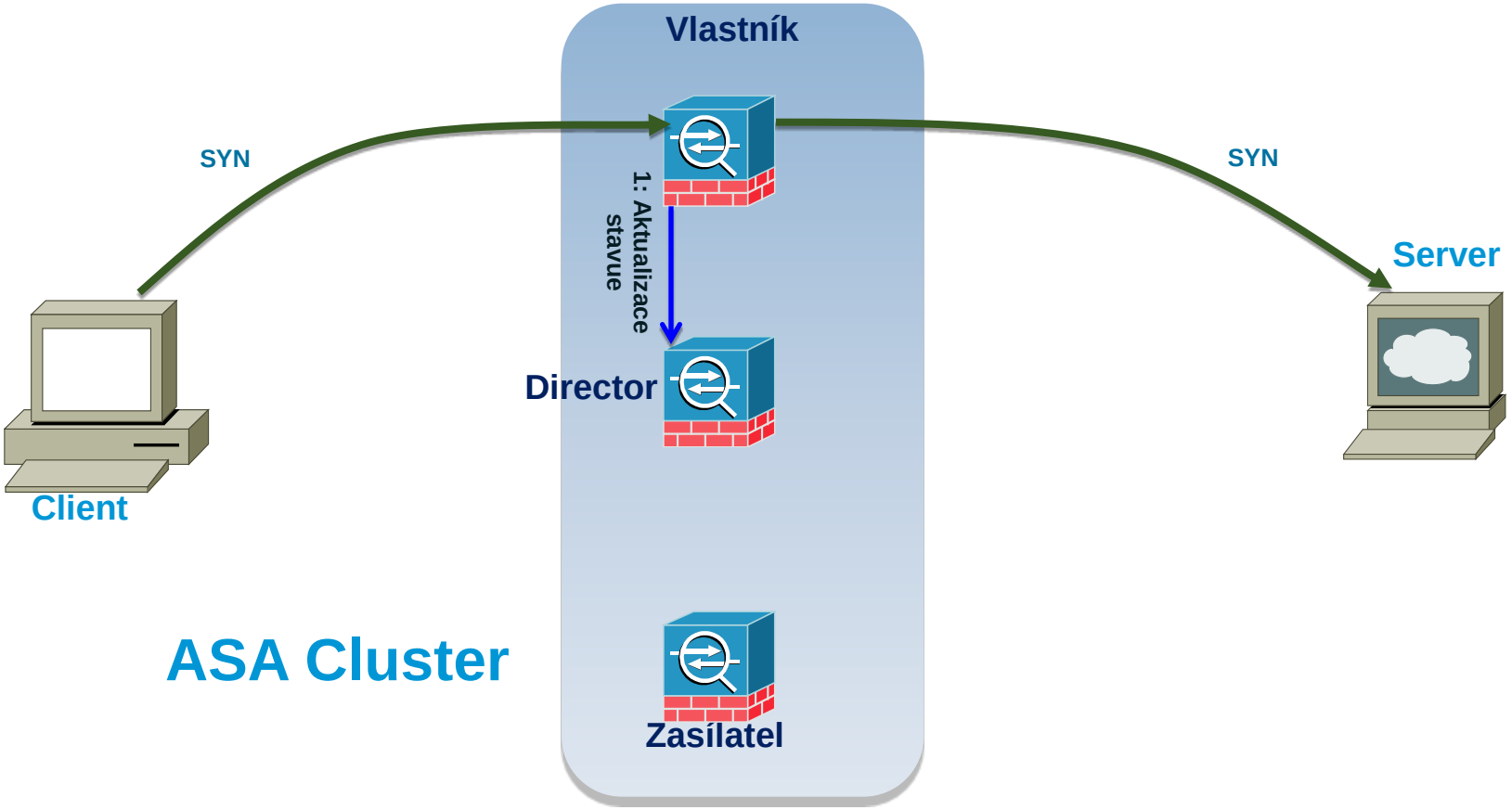
Počet spojení za sekundu
350,000 CPS

Funkce
FW, IPS, vzdálený přístup

Modularita, pružnost nasazení

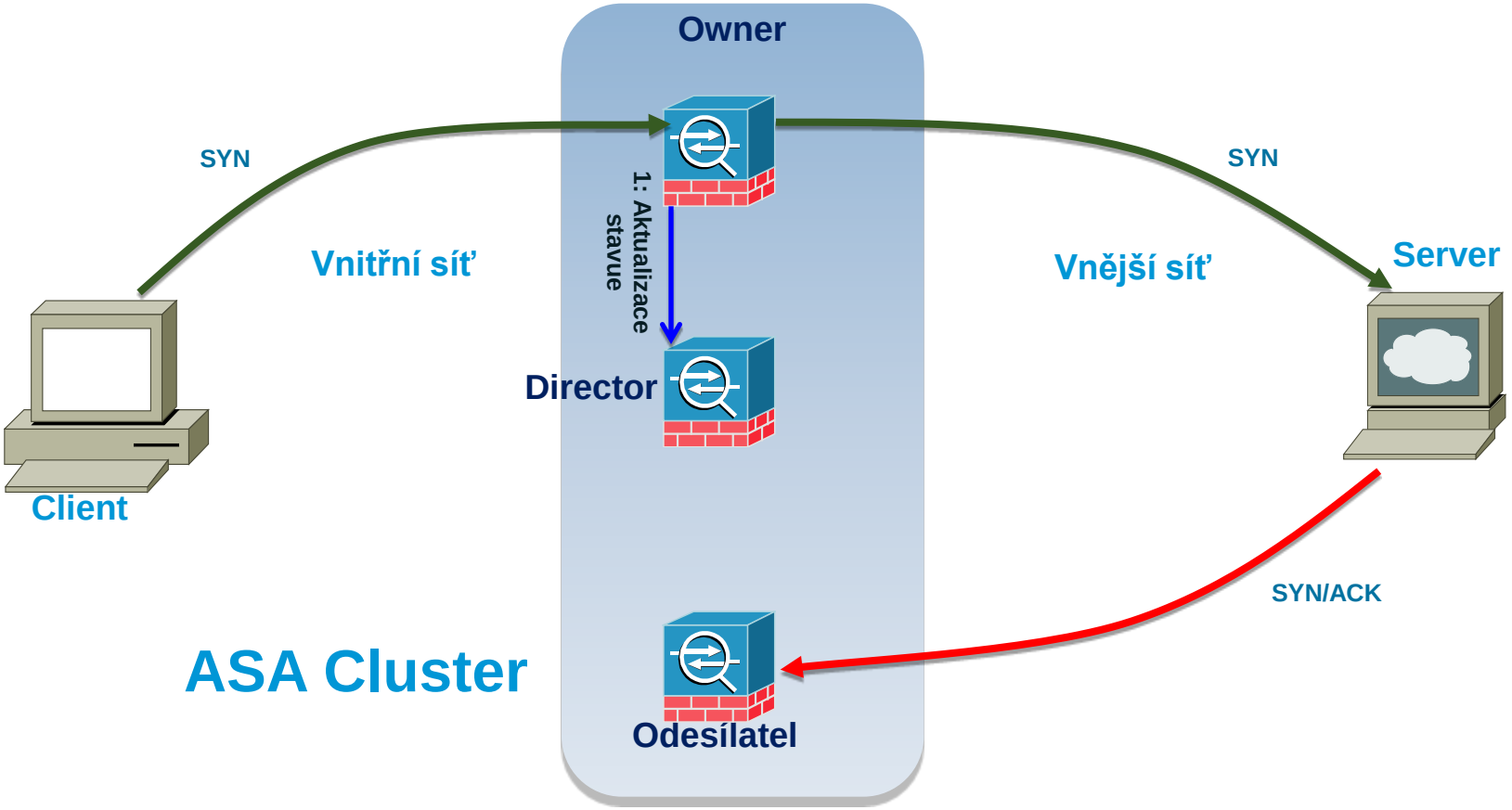
Propustnost
Až 40 Gbps FW
10 Gbps IPS

ASA 5585-X MultiScale Cluster



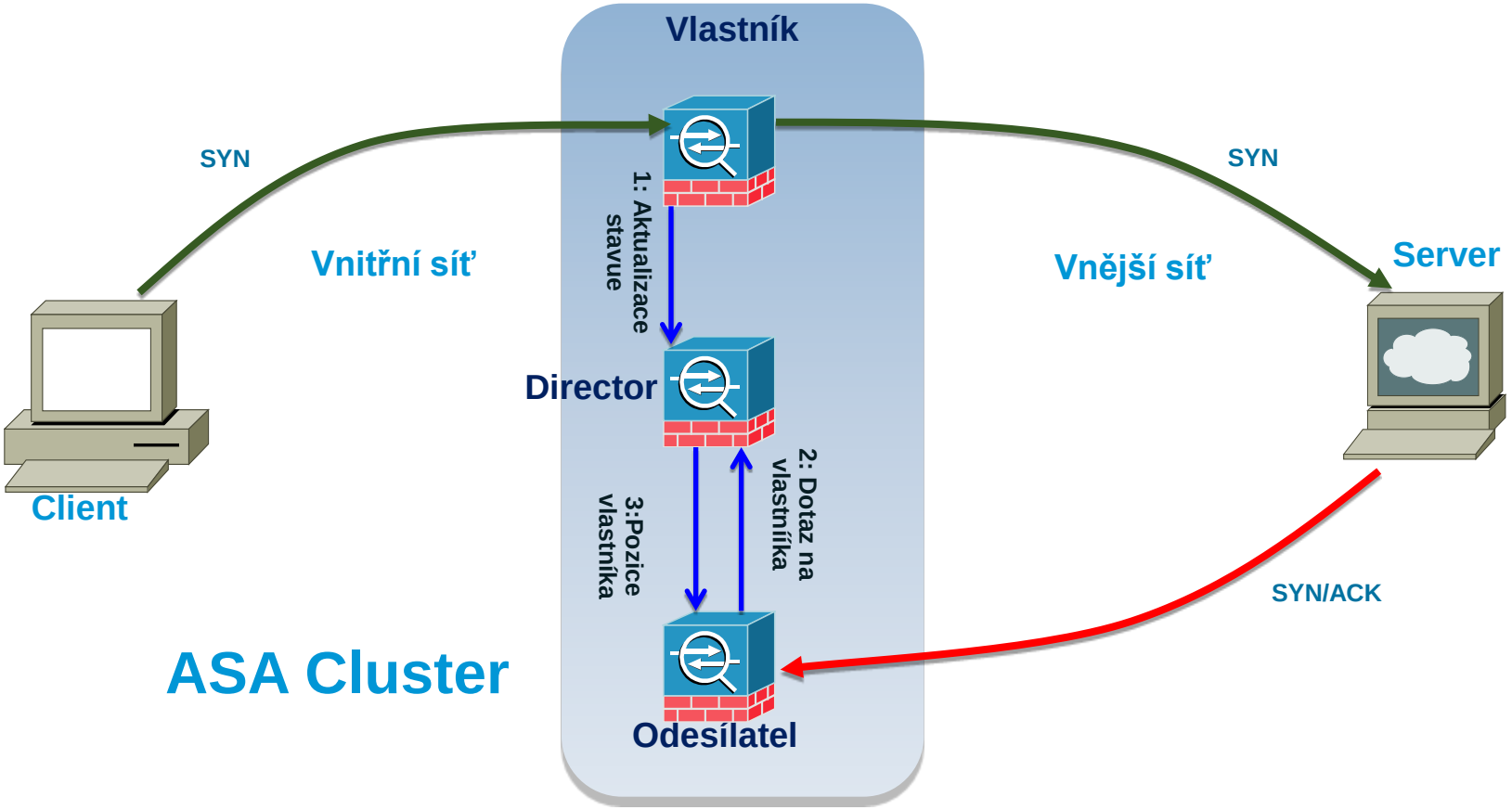
- Director je zvolen per spojení pomocí hashing algoritmu
- Director slouží jako záloha pro případ selhání vlastníka
- Optimalizace může vypustit kroky 2 a 3 pokud je to potřeba

ASA 5585-X MultiScale Cluster



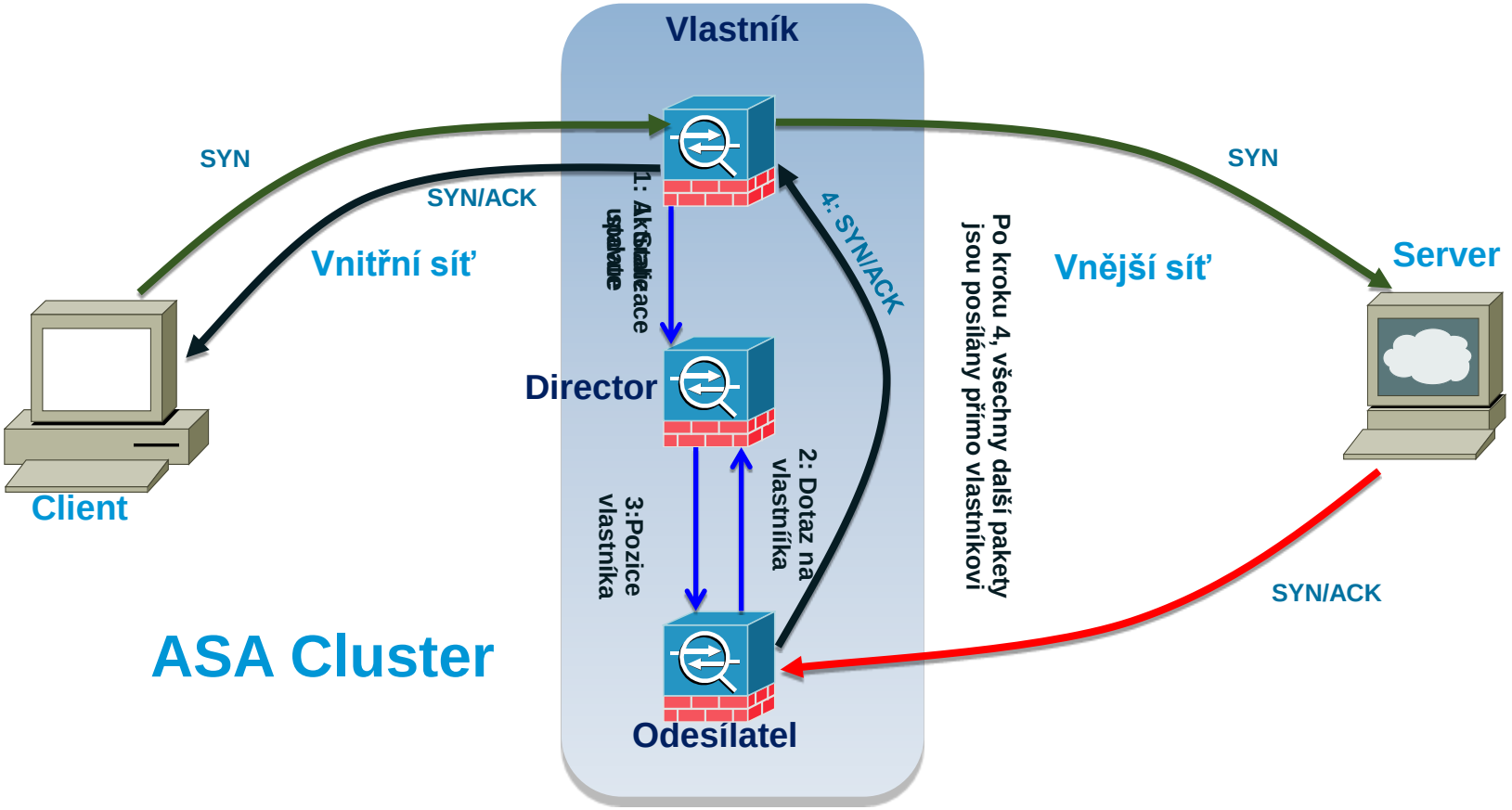
- Director je zvolen per spojení pomocí hashing algoritmu
- Director slouží jako záloha pro případ selhání vlastníka
- Optimalizace může vypustit kroky 2 a 3 pokud je to potřeba

ASA 5585-X MultiScale Cluster



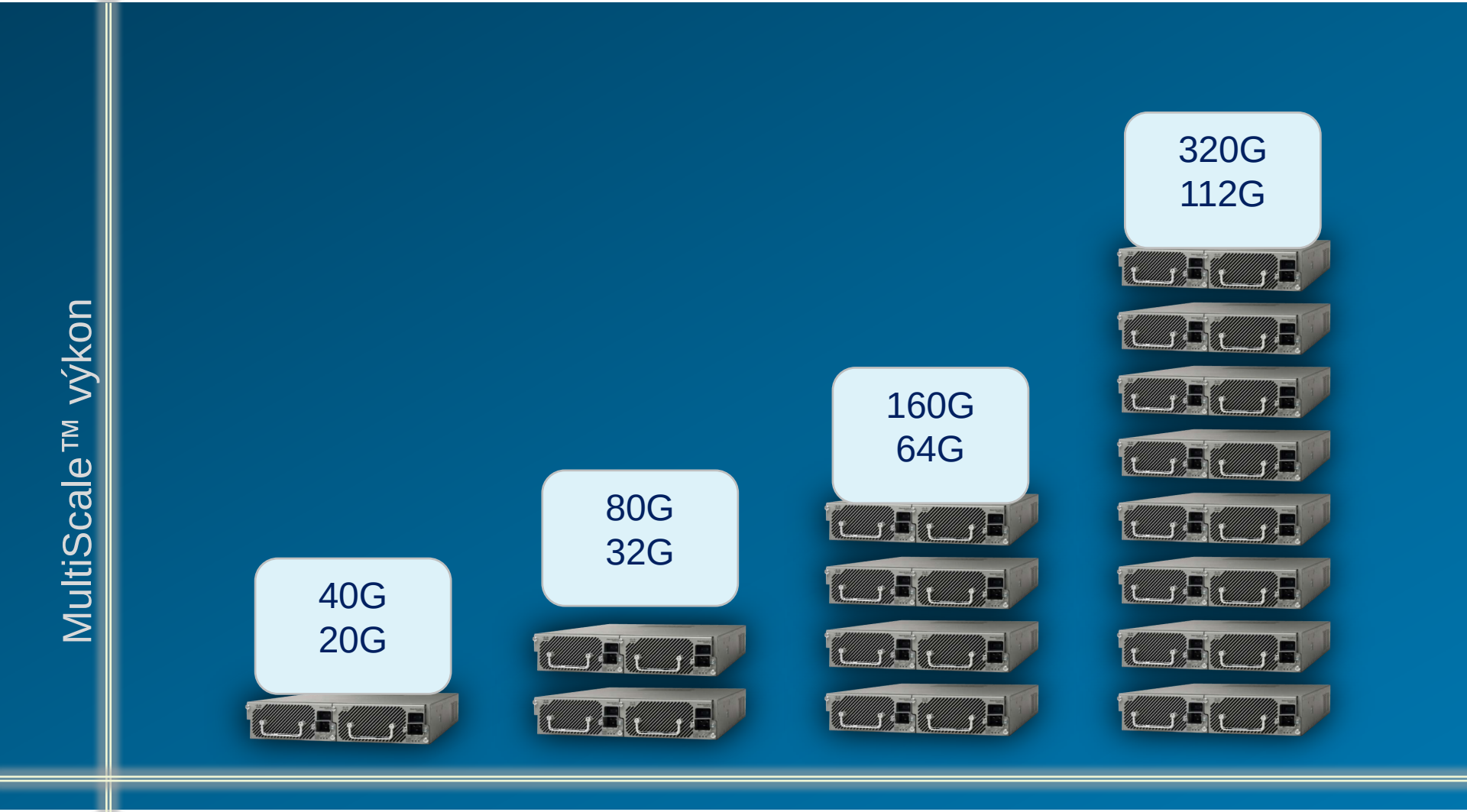
- Director je zvolen per spojení pomocí hashing algoritmu
- Director slouží jako záloha pro případ selhání vlastníka
- Optimalizace může vypustit kroky 2 a 3 pokud je to potřeba

ASA 5585-X MultiScale Cluster



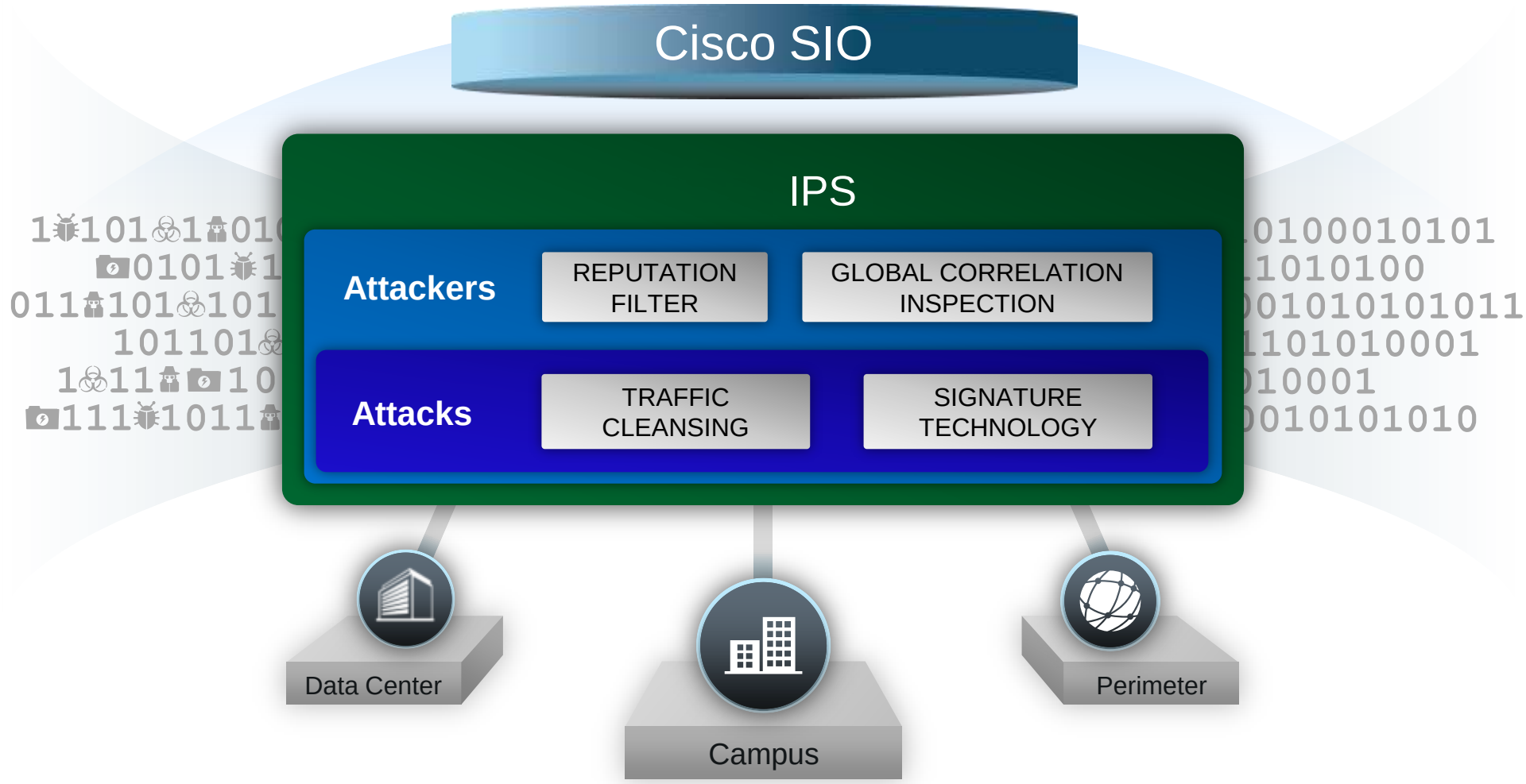
- Director je zvolen per spojení pomocí hashing algoritmu
- Director slouží jako záloha pro případ selhání vlastníka
- Optimalizace může vypustit kroky 2 a 3 pokud je to potřeba

Až ke 300G firewallu (MultiScale™)

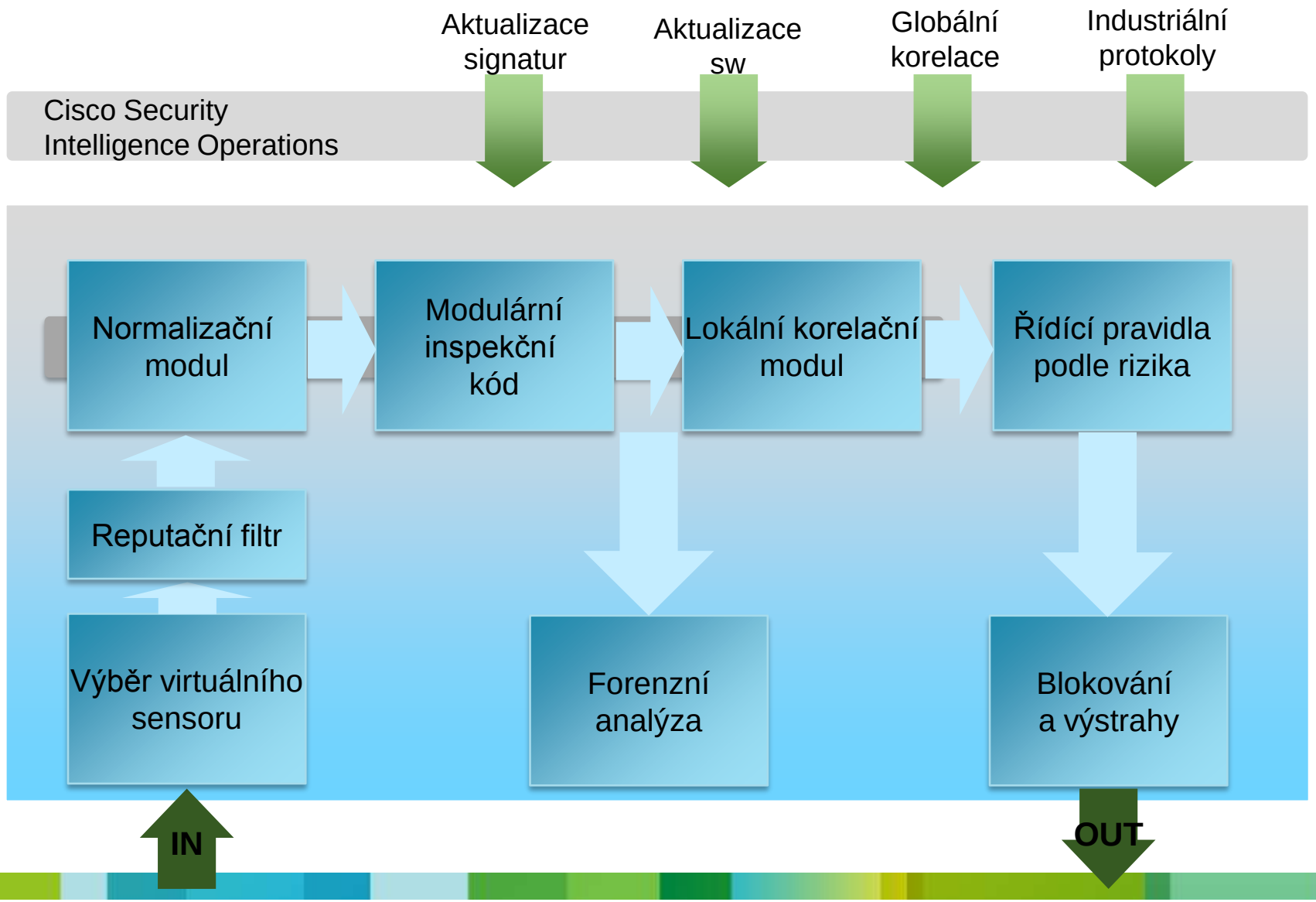


Cisco IPS

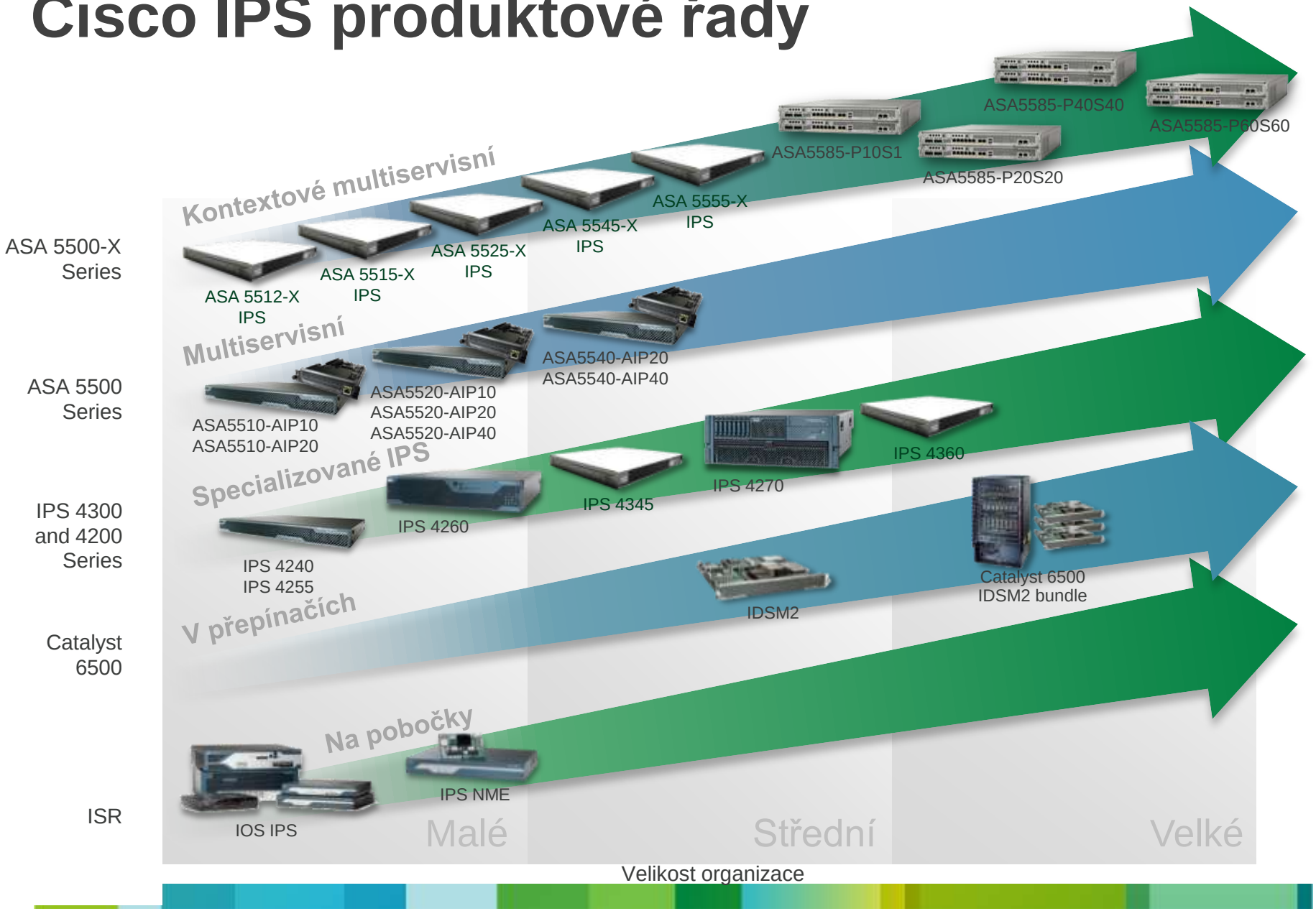
Innovations in Threat Management



Cisco IPS architektura



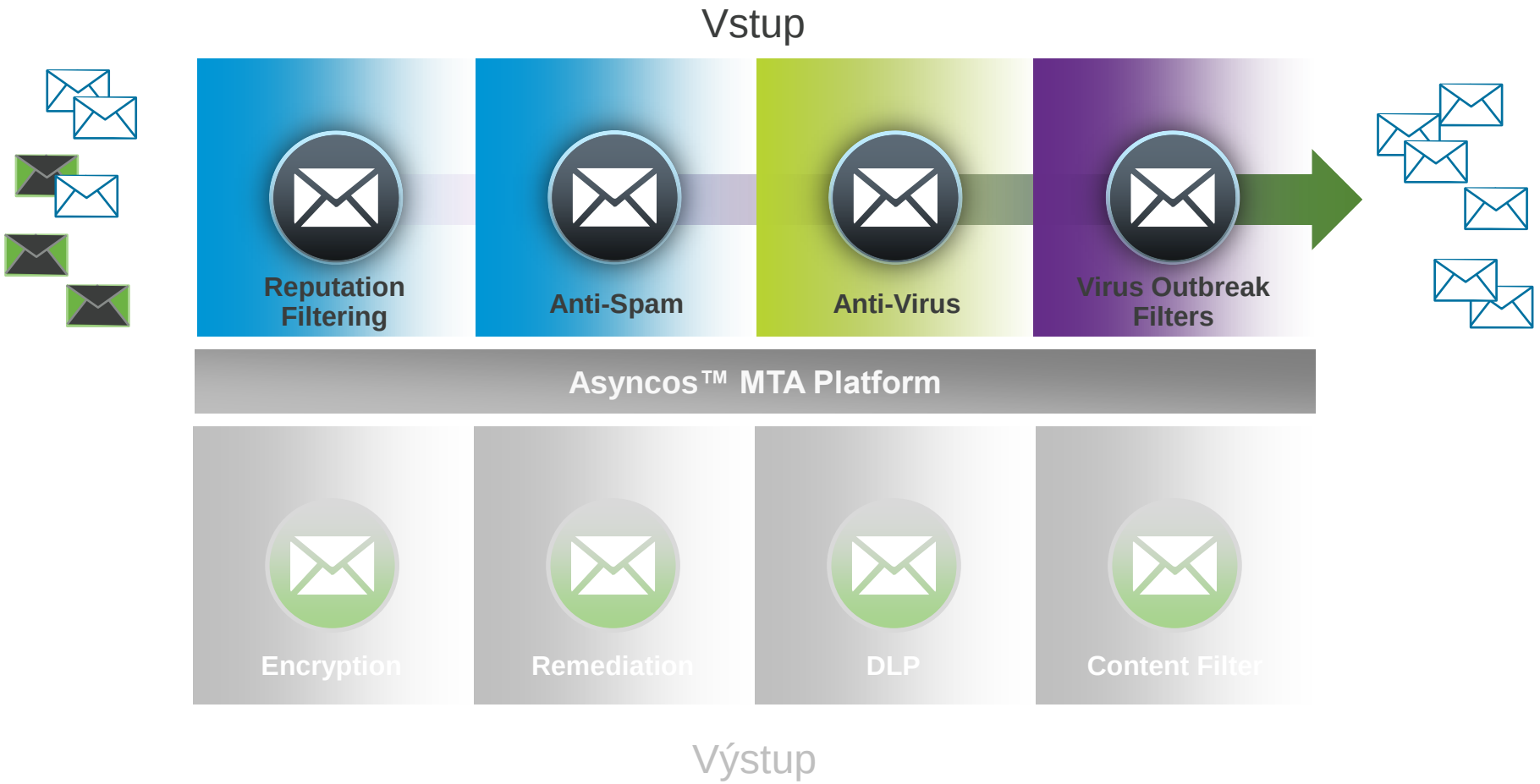
Cisco IPS produktové řady



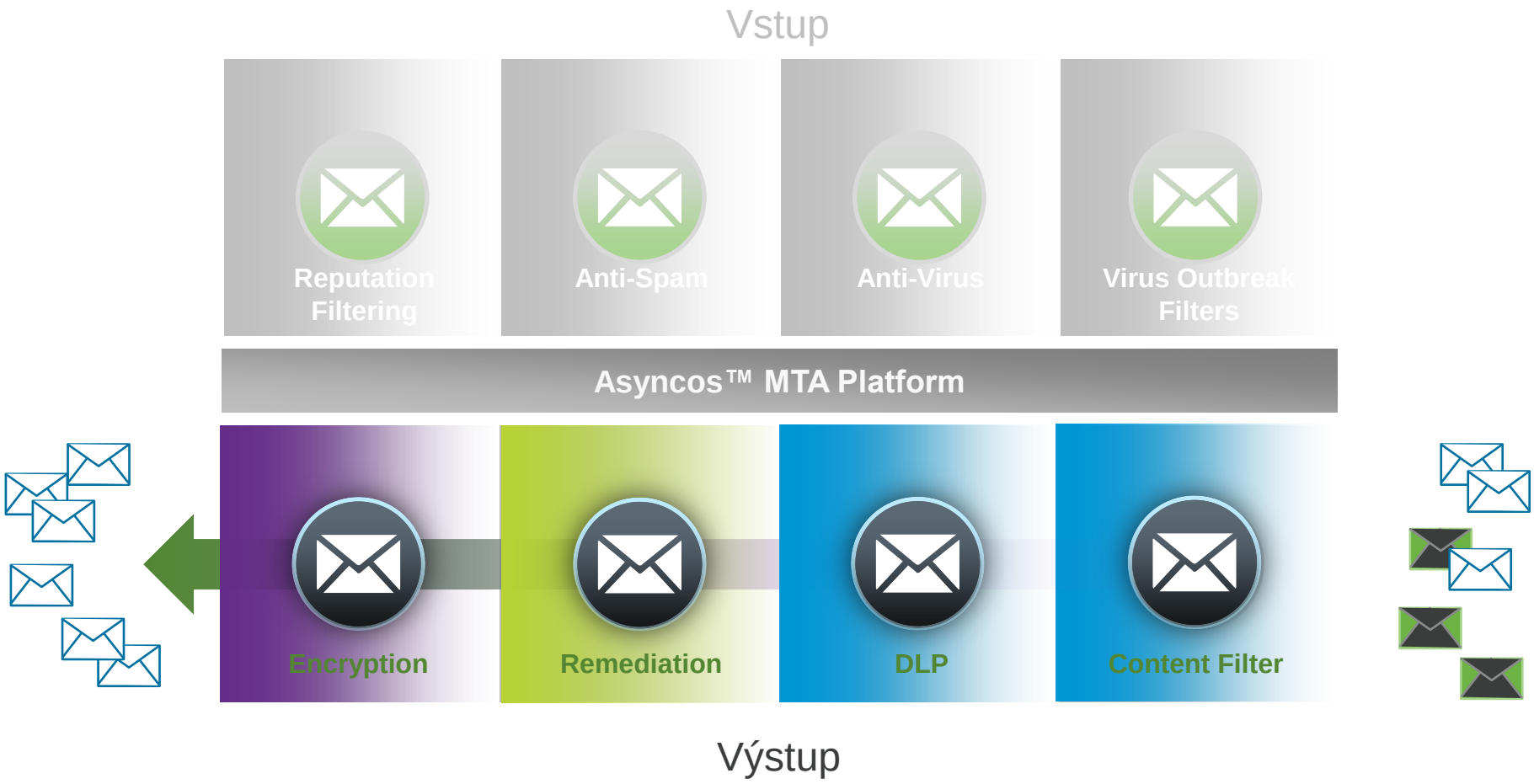
Ochrana web komunikace

Ochrana e-mail komunikace

Vícevrstvá ochrana na vstupu



Vícevrstvá ochrana na výstupu



Cisco SecureX řešení

Dynamické prostředí podnikových sítí

Bezpečný přístup a jednotná pravidla

Rozlišení zařízení, uživatelů a rolí

ISE, VPN, ASA, MACSec, Síť, AnyConnect

Vzdálený přístup

Bezpečná mobilita

Rozšíření firemní sítě

ISE, MACSec, ScanSafe, VPN, AnyConnect, WSA

Útoky, malware

Síť a hranice sítě

Ochrana přenášených dat

ISE, Router, VPN, ASA, IPS, ESA

Virtualizace

Bezpečná datová centra a cloud

Ochrana mozku firmy

VPN, ASA, Nexus 1000V, VSG

Cisco SecureX

V kontextu je síla

ZABEZPEČENÍ:

Nexus 1000V

VSG

ASA

VPN

Bezpečná datová centra a cloud

OBTÍŽE

Snížená viditelnost dat

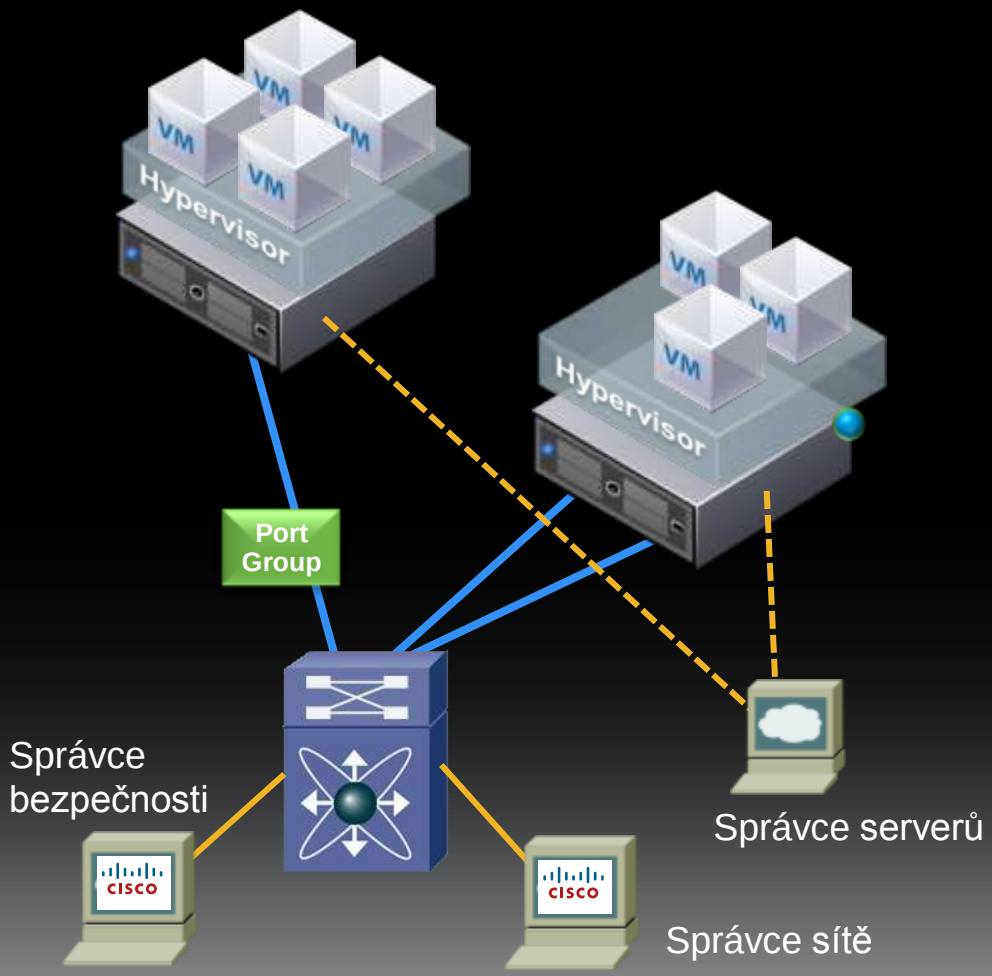
Nezabezpečená bílá místa

Menší zkušenost s novými technologiemi

Koordinace kompetencí

Rozšiřování kapacit bezpečnostních řešení

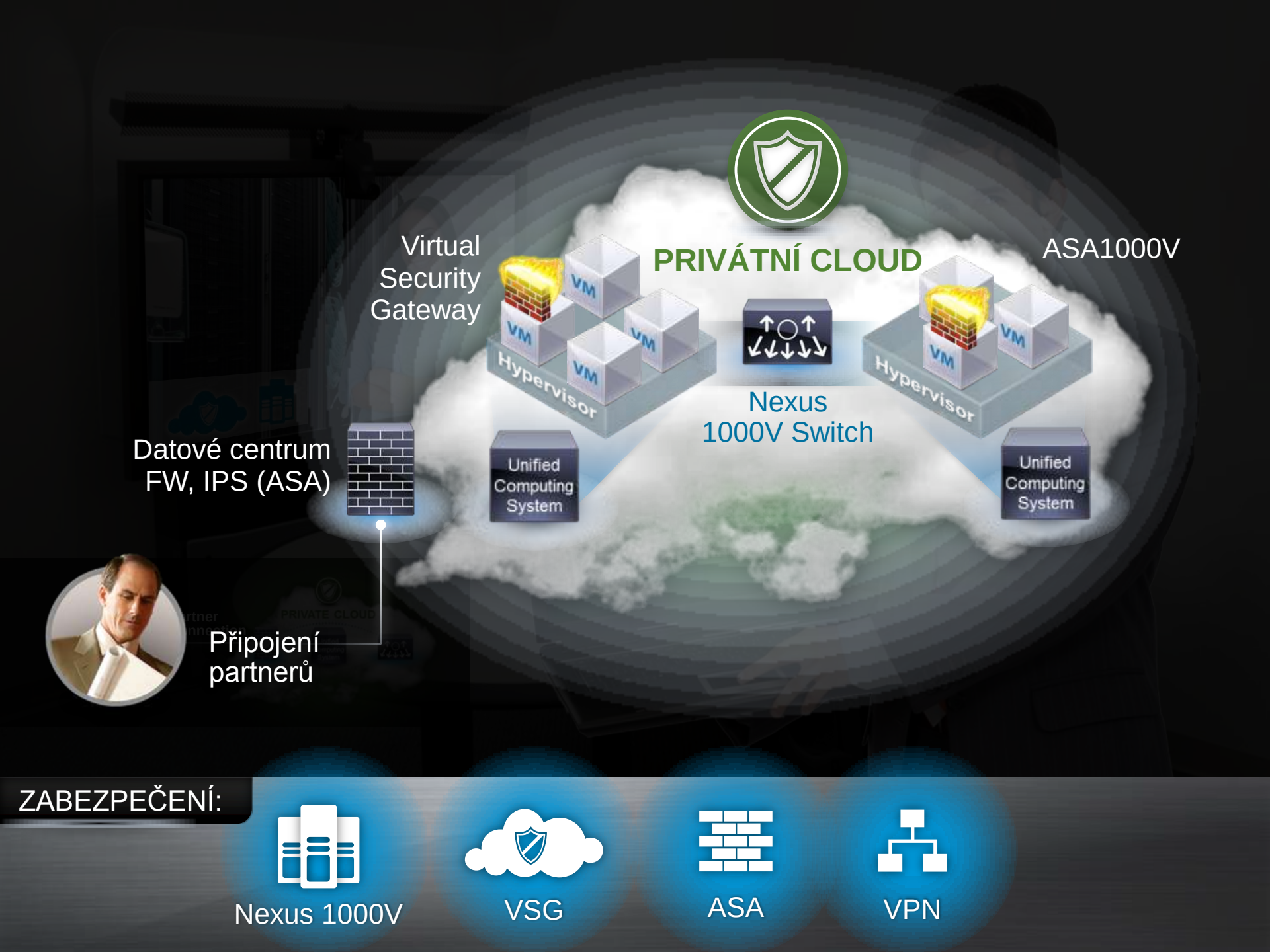
Virtualizace serverů ztěžuje zabezpečení



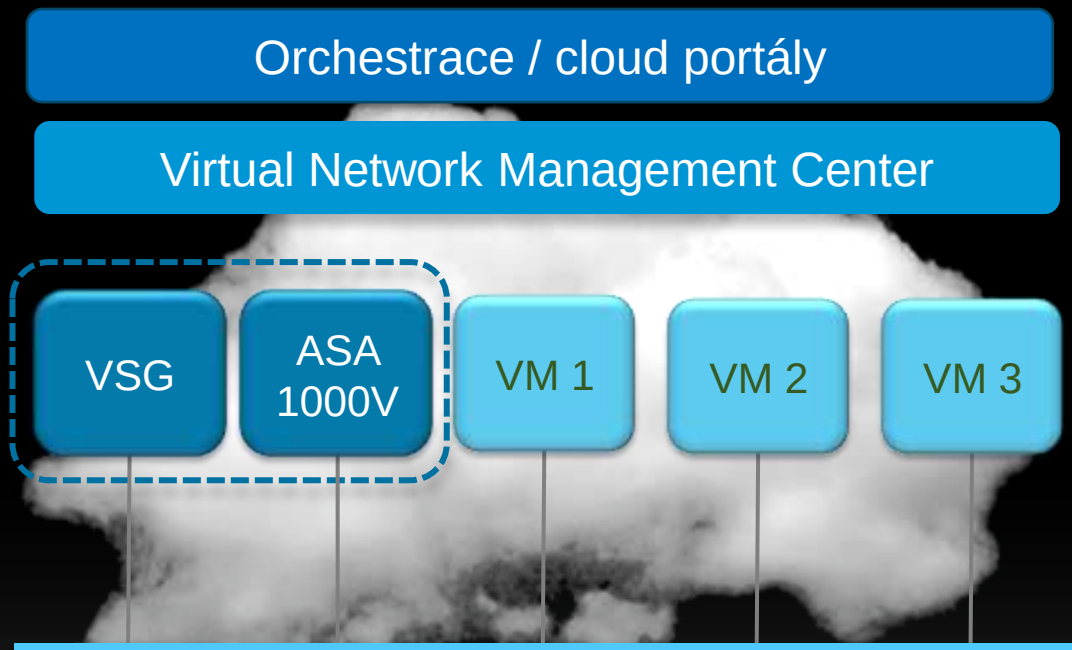
1. **vMotion přesouvá VM mezi fyzickými porty—pravidla v síti musí následovat vMotion (přes racky, řady, DCs)**

2. **Potřebujeme vidět lokálně přepínaná data a aplikovat na ně pravidla**

3. **Musíme zajistit oddělení rolí pro zachování nepřerušeného provozu**


Virtual
Security
Gateway
PRIVÁTNÍ CLOUD
ASA1000V
VM
VM
VM
VM
VM
VM
Hypervisor
Hypervisor
Nexus
1000V Switch
Unified
Computing
System
Unified
Computing
System
Datové centrum
FW, IPS (ASA)
Připojení
partnerů
ZABEZPEČENÍ:
Nexus 1000V
VSG
ASA
VPN

Architektura pro virtuální prostředí



Rozšiřuje existující ***pracovní postupy*** do virtuálního prostředí

Rozšiřuje ***síťové*** služby do virtuálního prostředí

Rozšiřuje ***síťovou*** infrastrukturu do virtuálního prostředí

Nexus 1000V

vPath

Výpočetní prostředí (e.g. UCS)

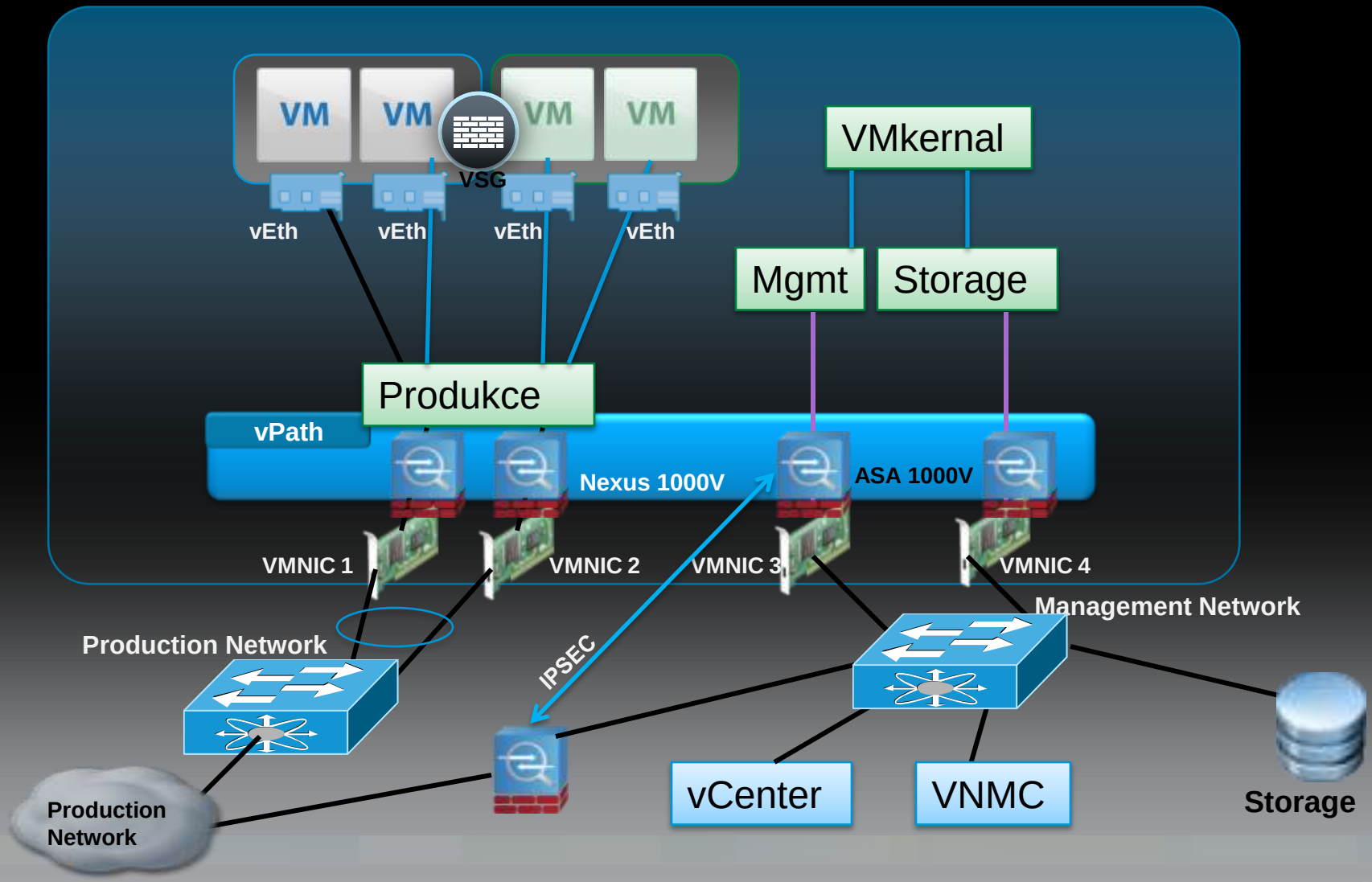
Virtualizované

Pružné

Řízené pravidly

Multi-tenant

Oddělení provozu v DC



VÝSLEDEK

Nexus 1000V

VSG

ASA

VPN

V CONTEXTU JE SÍLA !

Business pravidla

Kdo

Kdy

Jak

Kde

Kdy

Porozumění hrozbám

SensorBase

Operační středisko

Dyn. aktualizace

Prosazení v síti

V síťové infrastruktuře

Překryvné, výkonné

Připojené do cloudu

Děkuji