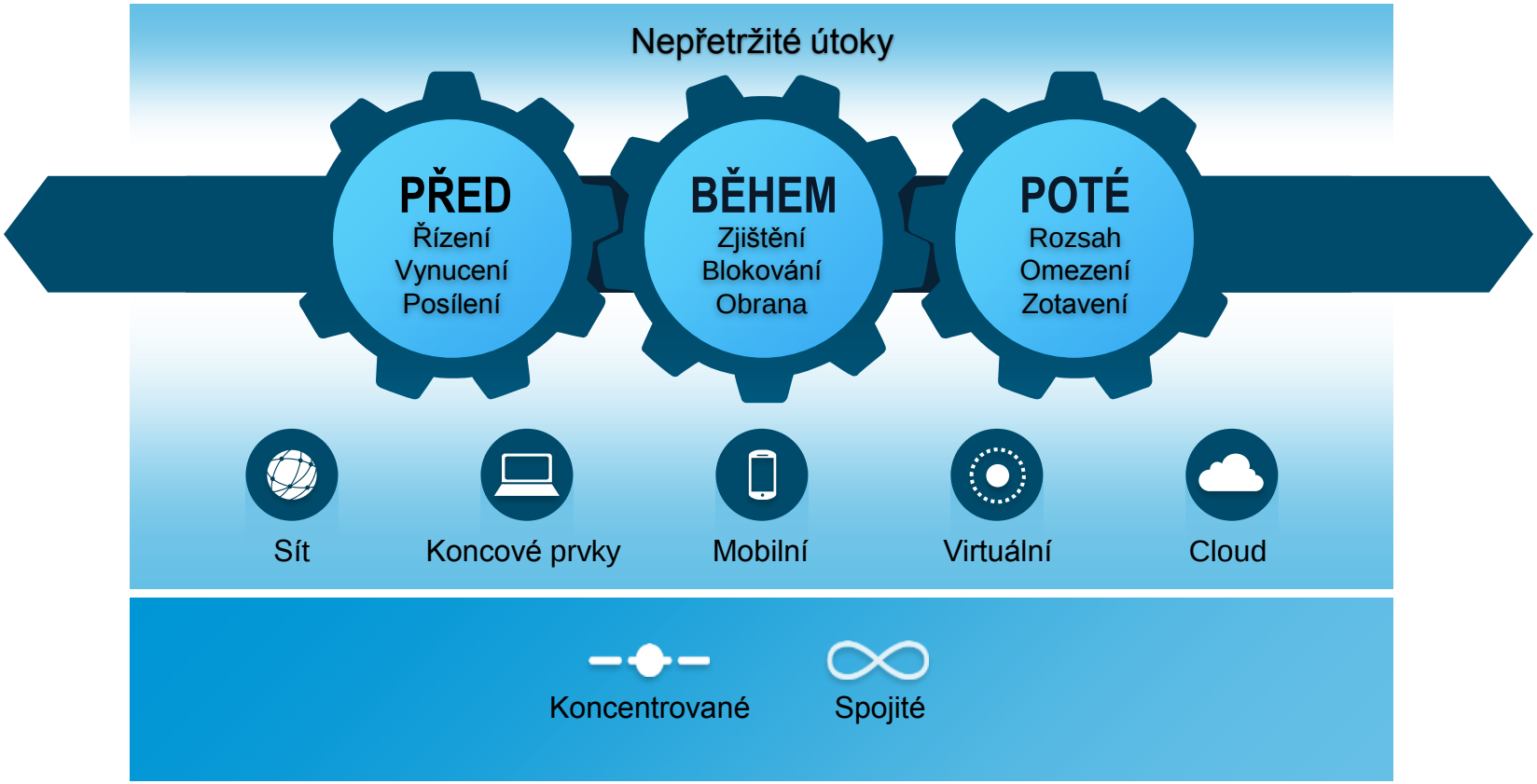
Úloha sítě při zajištění kybernetické bezpečnosti

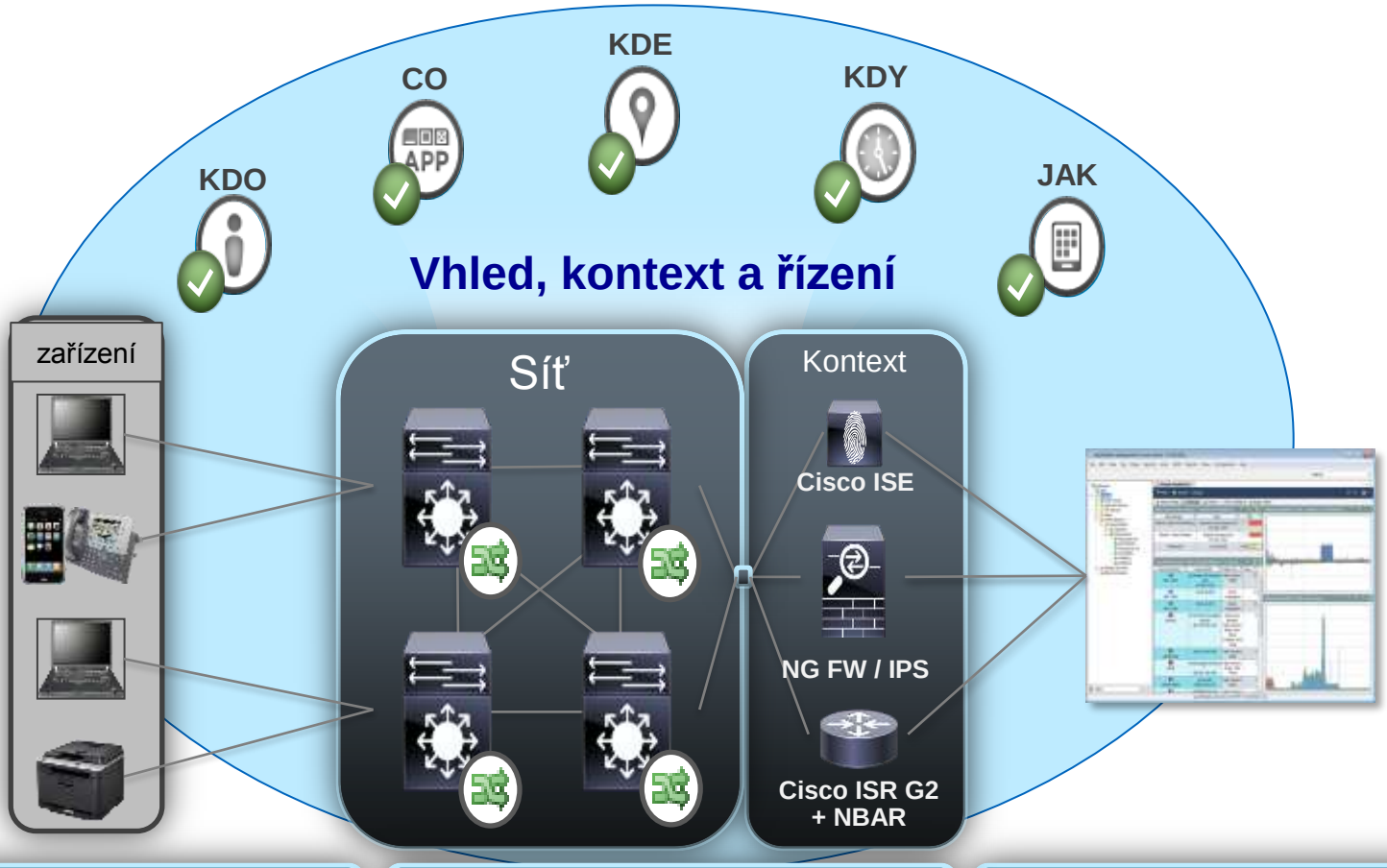
Ivo Němeček, CCIE #4108
Manager, Systems Engineering

Konference ISSS, 8. 4. 2014

Bezpečnostní model



Obrana v síti

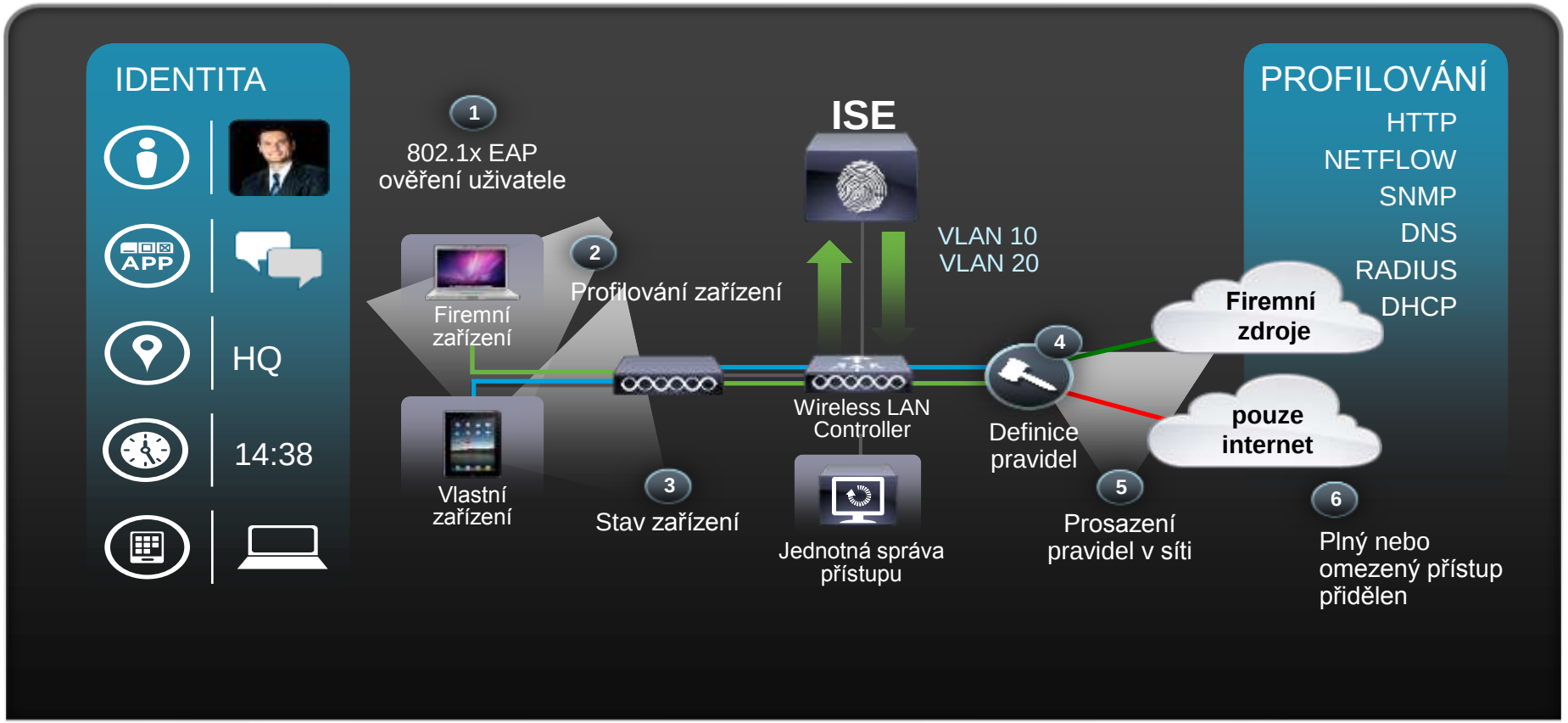


NetFlow Data pro vhled do komunikace od přístupové vrstvy

Obohacení Flow dat o identitu, událostí a aplikační info pro kontext

Jednotný pohled na síť pro detekci, vyšetřování a výkazy

Řízení přístupu do sítě podle kontextu



Rozpoznávání připojených zařízení

Řešení

ISE Profiler
+ IOS Sensor

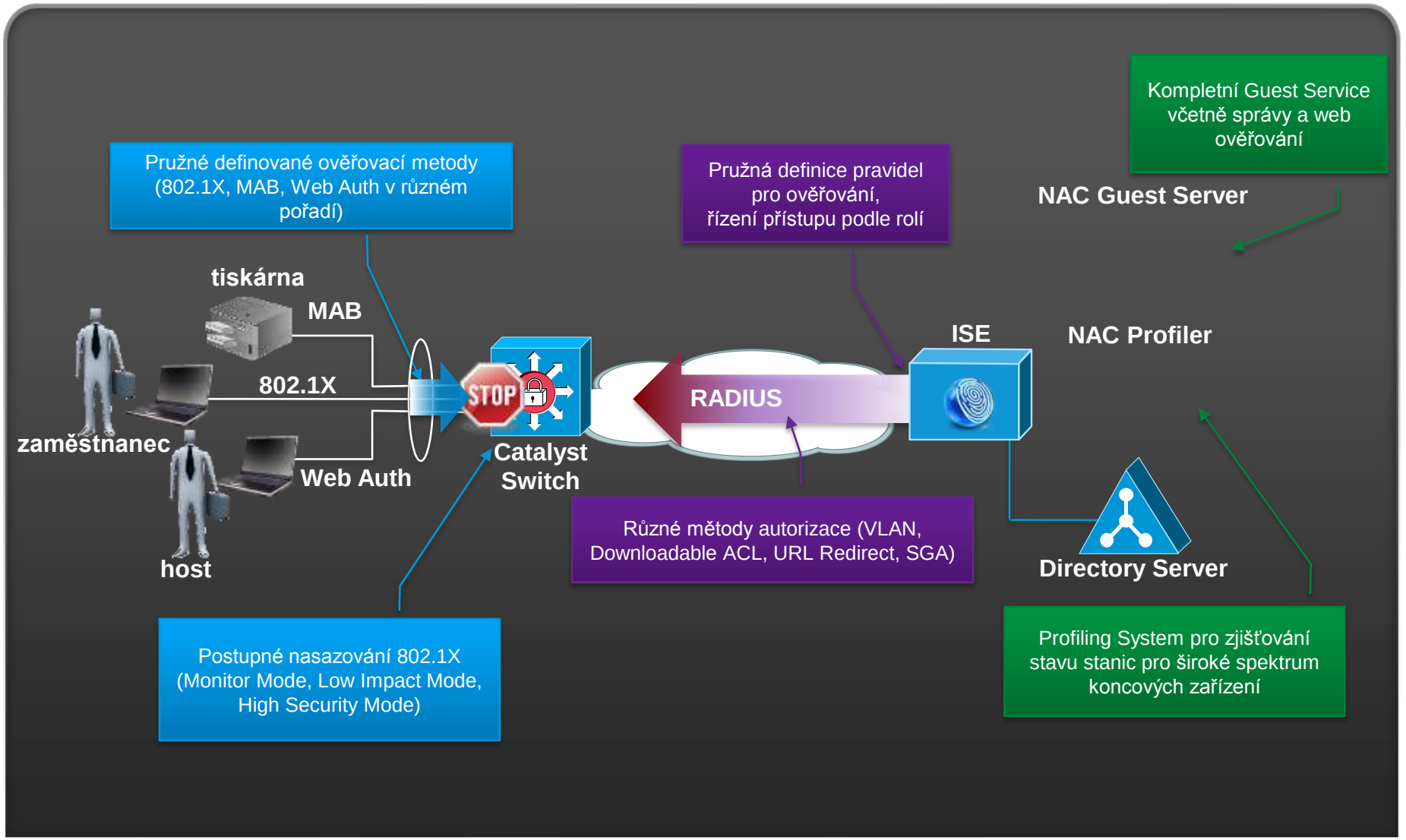
Typický scénář spolupráce ISE a Cisco IOS Sensor

Sběr dat – přepínač shromažďuje data týkající se zařízení a předává je do ISE

Klasifikace – ISE klasifikuje zařízení, shromažďuje informace o datovém toku a poskytuje informace o zařízení

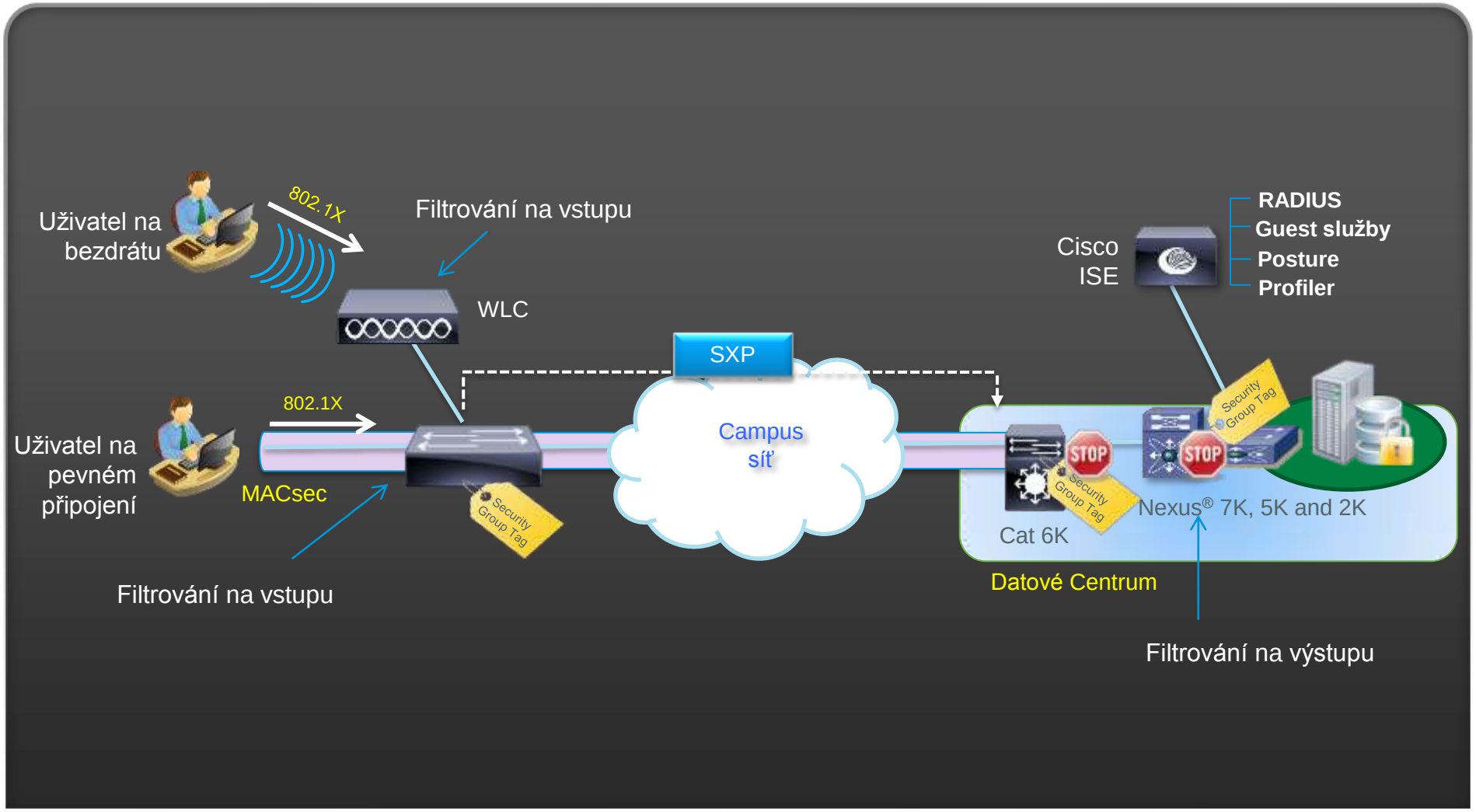
Autorizace – ISE uplatňuje pravidla podle vyprofilovaného kontextu

Přidělování oprávnění po ověření



Řízení v síti podle rolí

Trustsec

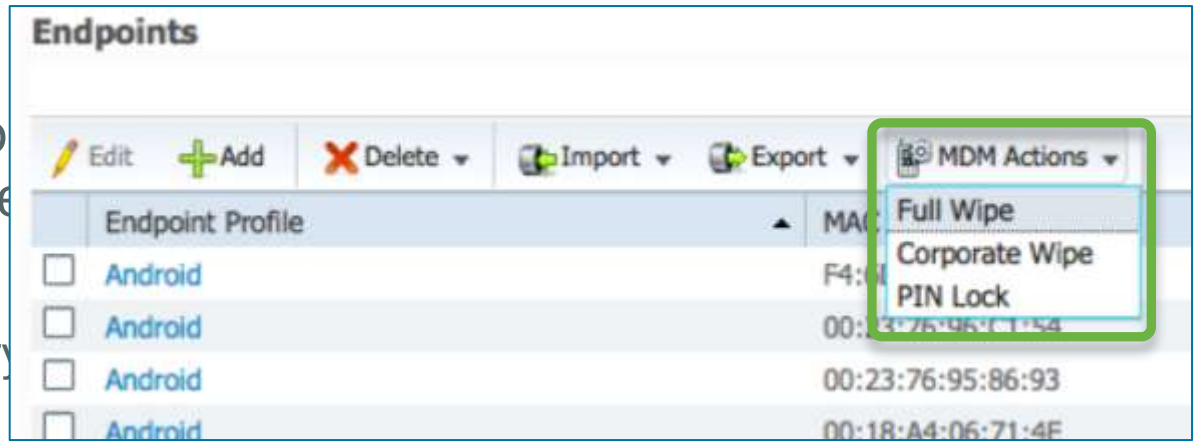


Autorizace

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Black List	If **Blacklist**	then Blackhole Traffic
✓	Profiled Cisco IP Phones ISE	If **Cisco-IP-Phone**	then Cisco_IP_Phones_ISE
✓	Printers	If **HP-Color-LaserJet-4700** OR **Xerox-Phaser-6010n**	then Printers
✓	Corp Workstation	If (Wireless_Access_ISE AND Wired_802.1X_ISE AND CorpAD:ExternalGroups EQUALS cisco.com/Users/Domain Computers AND Network Access:EapTunnel EQUALS EAP-FAST AND Network Access:EapAuthentication EQUALS EAP-TLS AND Network Access:EapChainingResult EQUALS User failed and machine succeeded AND Session:PostureStatus EQUALS Compliant AND NewYork)	then AD_Login
✓	Employee and Corp_Workstation	If (Wireless_Access_ISE AND Wired_802.1X_ISE AND CorpAD:ExternalGroups EQUALS cisco.com/Users/Domain Users AND Network Access:EapTunnel EQUALS EAP-FAST AND Network Access:EapAuthentication EQUALS EAP-TLS AND Network Access:EapChainingResult EQUALS User and machine both succeeded AND Session:PostureStatus EQUALS Compliant AND NewYork)	then Employee
✓	Registered Devices	If **RegisteredDevices** AND (Wired_802.1X_ISE AND Network Access:EapAuthentication EQUALS EAP-TLS AND CERTIFICATE:Subject Alternative Name EQUALS Radius:Calling-Station-ID)	then BYOD Access
✓	Personal Devices	If **Employee** AND Network Access:EapAuthentication EQUALS EAP-MSCHAPv2	then BYOD Provisioning
✓	VPN	If VPN	then VPN Employee
✓	Guest	If **Guest** AND Bussiness Hours	then Internet Only
✓	Default	If no matches, then DenyAccess	

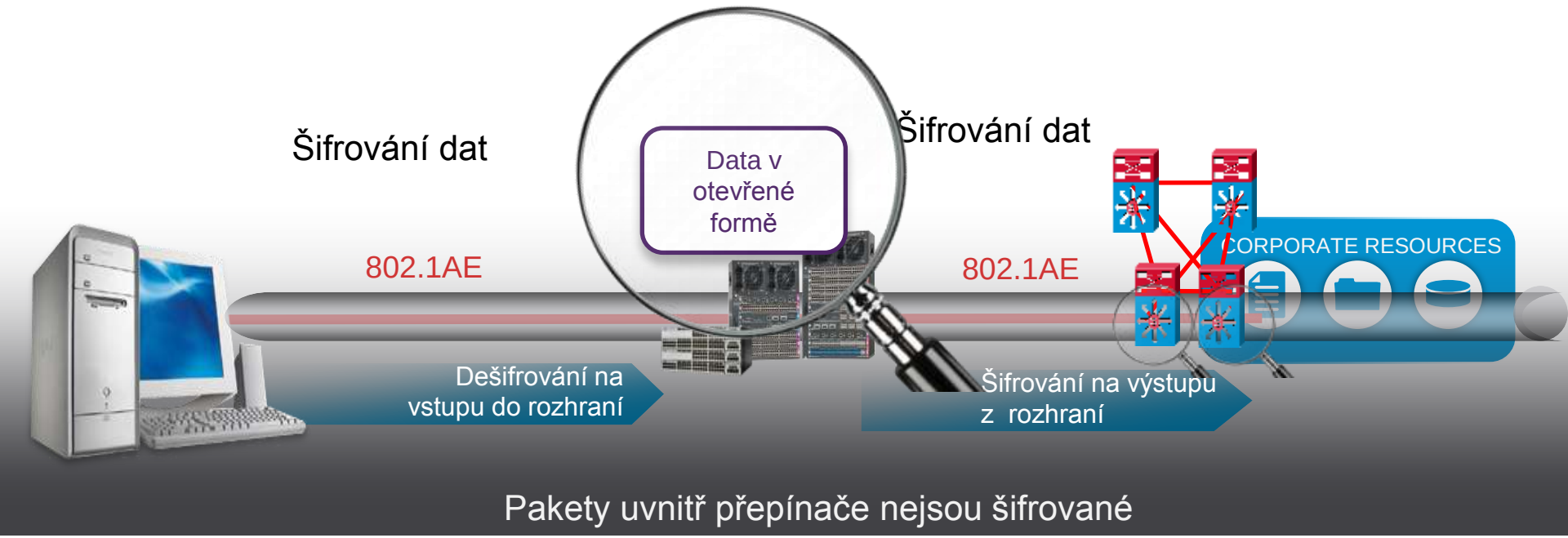
Integrace s MDM

- Administrátor může p
  zařízení přes MDM se
  - MyDevices Portal
  - ISE Endpoints Directory



Důvěrnost přenosů i v LAN sítích

Ochrana dat pomocí šifrování L2 (MACSec)



Řešení

Důvěrnost dat se zachovanou viditelností datových toků

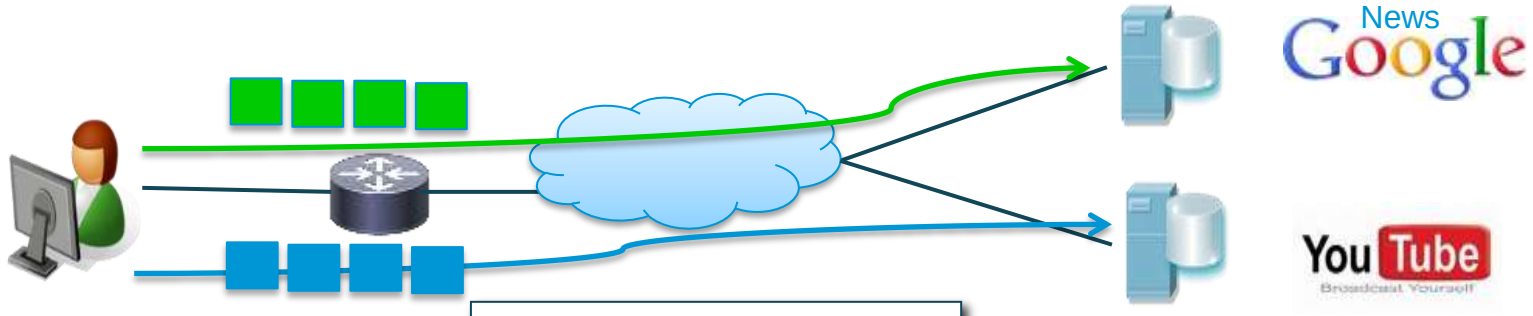
Typický scénář nasazení

Šifrování na L2 – „Hop by Hop”

Viditelnost datových toků pro uplatňování bezpečnostních pravidel a QoS

Monitorování toků v síti

Flexible NetFlow a NBAR



Key Fields	Packet #1
Source IP	10.1.1.1
Destination IP	173.194.34.13
Source Port	20457
Destination Port	23
Layer 3 protocol	6
TOS byte	0
Ingres Interface	Ethernet 0

```
flow record app_record
  match ipv4 source address
  match ipv4 destination address
  match …..
  match application name
```

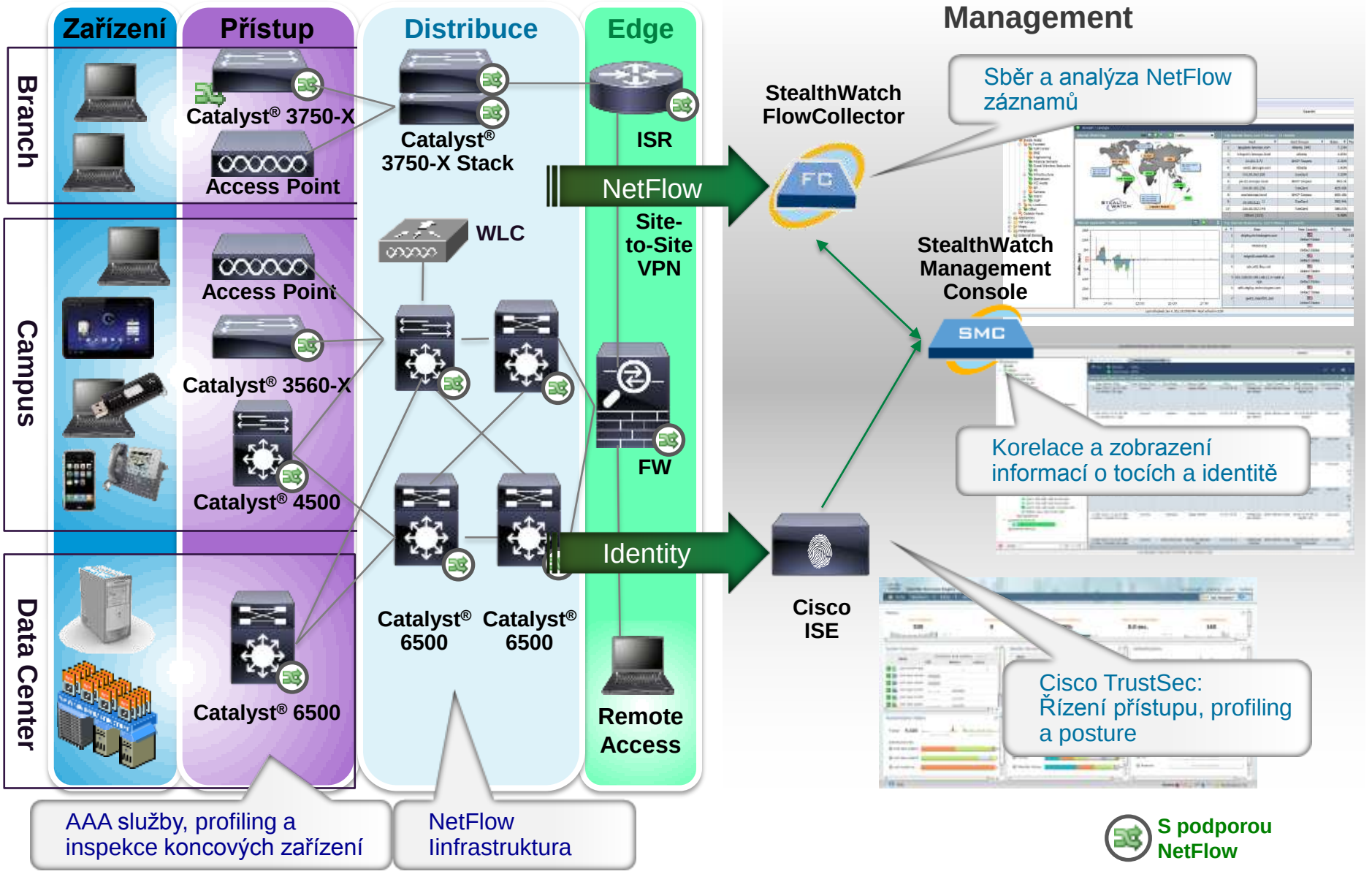
Key Fields	Packet #2
Source IP	10.1.1.1
Destination IP	72.163.4.161
Source Port	30307
Destination Port	80
Layer 3 protocol	6
TOS byte	0
Ingres Interface	Ethernet 0

NetFlow cache

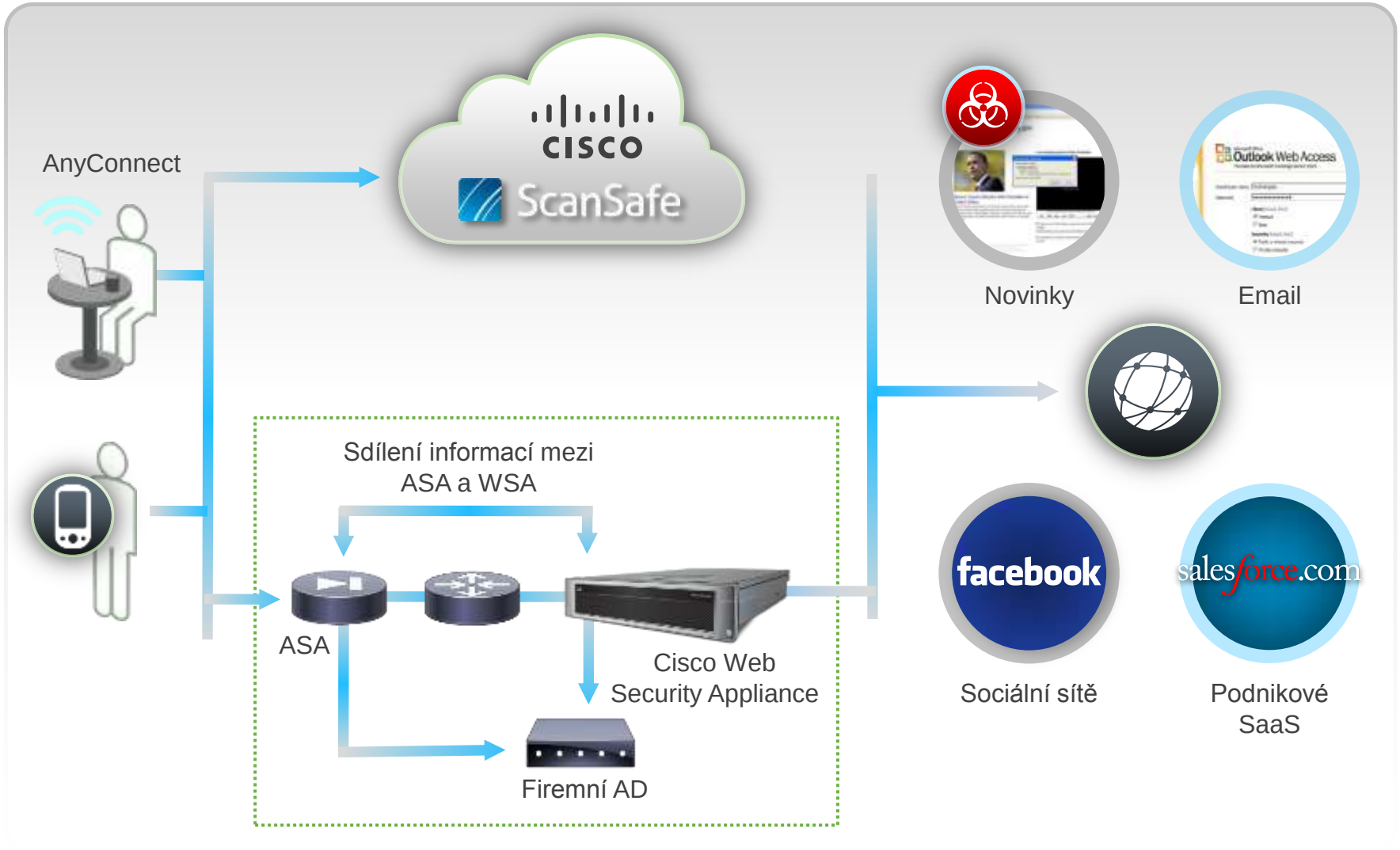
Src. IP	Dest. IP	Src. Port	Dest. Port	Layer 3 Prot.	TOS Byte	Ingress Intf.	App Name	Times tamps	Byttes	Packets
10.1.1.1	173.194.34.134	20457	80	6	0	Ethernet 0	**HTTP**			
10.1.1.1	72.163.4.161	30307	80	6	0	Ethernet 0	**Youtube**			

First packet of a flow will create the Flow entry using the Key Fields"
Remaining packets of this flow will only update statistics (bytes, counters, timestamps)

Architektura řešení Cyber Threat Defense



Hybridní ochrana web komunikace
s AnyConnect klientem



Centralizovaná inteligence
Security Intelligence Operations (SIO)

Centralizované řízení bezpečnosti
SDN přístupem

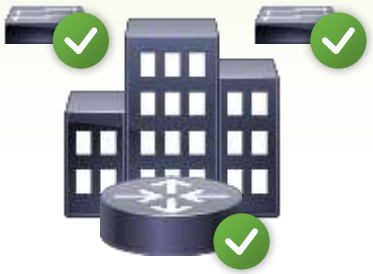
POKYN K NÁPRAVĚ

Defense Center

Cisco APIC
Enterprise Module

AKTUALIZACE

ZJIŠTĚNA HROZBA



Shrnutí: moderní síť…

- Chrání sebe samu i připojené stanice
- Řídí přístup ke informacím podle kontextu
- Chrání komunikaci šifrováním
- Obsahuje a využívá pokročilé bezpečnostní funkce (FW, IPS,…)
- Vidí hluboko i do šíře do komunikace
- Poskytuje cenné telemetrické údaje
- Spolupracuje se specializovanými bezpečnostními systémy
  - Přesměrovává k nim data
  - Vyměňuje si s nimi informace
  - Aktivně reaguje na hrozby

V KONTEXTU JE SÍLA !

Business pravidla

Kdo

Kdy

Jak

Kde

Kdy

Porozumění hrozbám

Globální inteligence

Operační středisko

Dyn. aktualizace

Prosazení v síti

V síťové infrastruktuře

Překryvné, výkonné

Připojené do cloudu

Děkuji