

Jednotné řízení přístupu do sítě v prostředí BYOD

Pavel Křižanovský

Customer Solutions Architect

Cisco Systems Česká Republika

pkrizano@cisco.com



Agenda

- Úvod
- Důsledky BYOD pro IT
- Cisco řešení pro BYOD
- Závěr



Agenda

- Úvod
- Důsledky BYOD pro IT
- Cisco řešení pro BYOD
- Závěr



IT prostředí se mění...





BYOD = Bring Your Own Device

Přines si Své Vlastní Zařízení



Nová očekávání uživatelů

Vývoj požadavků na pracovní prostředí

NÁRŮST POČTU ZAŘÍZENÍ

Do roku 2015 bude
do sítě připojeno 15
miliard zařízení



Každá osoba bude mít
průměrně 3-4 zařízení
připojovaná do sítě



40% zaměstnanců bude nosit
svá zařízení do práce



NÁRŮST POČTU
ZAŘÍZENÍ

NOVÁ GENERACE
PRACOVNÍKŮ

VIRTUALIZACE

Nová očekávání uživatelů

Vývoj požadavků na pracovní prostředí

NOVÁ GENERACE PRACOVNÍKŮ

“Práce” již neoznačuje
místo, kde se pracuje

Lidé jsou ochotni si nechat
snížit plat, budou-li mít
možnost pracovat z domova

70% procent koncových
uživatelů přiznává, že
občas porušuje firemní IT
politiku za účelem
zjednodušení svých aktivit

Odkudkoliv, kdykoliv, z jakéhokoliv zařízení



NÁRŮST POČTU
ZAŘÍZENÍ

NOVÁ GENERACE
PRACOVNÍKŮ

VIRTUALIZACE

Nová očekávání uživatelů

Vývoj požadavků na pracovní prostředí

VIRTUALIZACE

“60% serverů bude do konce 2013 virtualizováno”

“20% profesionálních PC bude do konce roku 2013 provozováno jako virtuální desktop.”

Rozvoj datacenter, aplikace se stávají objekty migrujícími skrze síť



NÁRŮST POČTU
ZAŘÍZENÍ

NOVÁ GENERACE
PRACOVNÍKŮ

VIRTUALIZACE



Agenda

- Úvod
- **Důsledky BYOD pro IT**
- Cisco řešení pro BYOD
- Závěr

Důsledky BYOD

Nové nároky na IT



- Jak eliminuji risk vyplývající z připojení soukromého uživatelského zařízení?
- Jak zajistím konzistentní uživatelské prostředí na všech zařízeních?
- Jak implementuji bezpečnostní politiku v závislosti na identitě uživatele a zařízení?
- Pro co a jak budu zajišťovat podporu?

Nárůst počtu zařízení

Důsledky BYOD

Nové nároky na IT



- Nebráním svým zaměstnancům ve zdravé soutěživosti?
- Udržím nejtalentovanější zaměstnance?
 - Jak zajistím splnění firemních předpisů?
- Zajišťuji dostatečné podmínky pro kontraktory, partnery a hosty?

Nová generace pracovníků

Důsledky BYOD

Nové nároky na IT



- Jak se dozvím, kdo přistupuje k mnou spravovaným virtuálním desktopům?
- Jak škálovatelným způsobem zajistím svým uživatelům přístup k datům v cloudu?
- Mohu zajistit plnění politik nezávisle na fyzickém umístění?

Virtualizace

Oblasti řešení komunikační bezpečnosti BYOD souvisí se vším

Dynamické prostředí sítí organizací

Bezpečný přístup
a jednotná pravidla



Rozlišení zařízení,
uživatelů a rolí

Vzdálený přístup

Bezpečná mobilita



Rozšíření sítě
organizace

Útoky, malware

Síť a hranice sítě



Ochrana
přenášených dat

Virtualizace

Bezpečná datová
centra a cloud



Ochrana mozku firmy

Typické způsoby nasazení BYOD



Restriktivní

Základní

Rozšířené

Plné

Prostředí vyžadující
přísnou kontrolu

Pouze firemní zařízení
Výroba
Citlivé obchodování
Klasifikované sítě státní
správy
Tradiční podniky

Základní služby a
jednoduchý přístup

Více typů zařízení,
pouze internet
Vzdělávací instituce
Veřejné instituce
Jednoduchý přístup pro
hosty

Různorodé aplikace,
bezpečná aktivace služeb

Více typů zařízení a
přístupových metod, VDI
Zdravotnictví
Podniky se zájmem o BYOD
Podpora kontraktorů

Široká podpora aplikací,
nové služby, plná kontrola

Více typů zařízení MDM
Inovativní firmy
Retail on Demand
Podpora mobilního prodeje
(Video, Collaboration, etc.)



Agenda

- Úvod
- Důsledky BYOD pro IT
- Cisco řešení pro BYOD
- Závěr

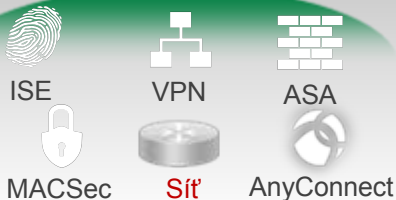
Cisco řešení kontextové bezpečnosti

Dynamické prostředí sítí organizací

Bezpečný přístup a jednotná pravidla



Rozlišení zařízení, uživatelů a rolí

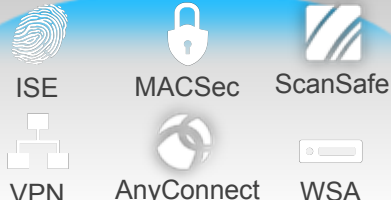


Vzdálený přístup

Bezpečná mobilita



Rozšíření firemní sítě

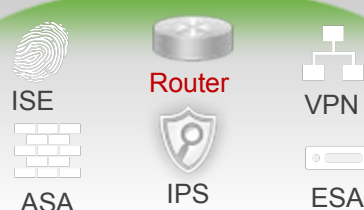


Útoky, malware

Síť a hranice sítě



Ochrana přenášených dat

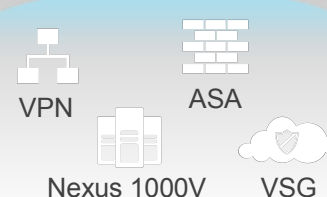


Virtualizace

Bezpečná datová centra a cloud



Ochrana mozku firmy



Cisco SecureX
V kontextu je síla



Bezpečný přístup



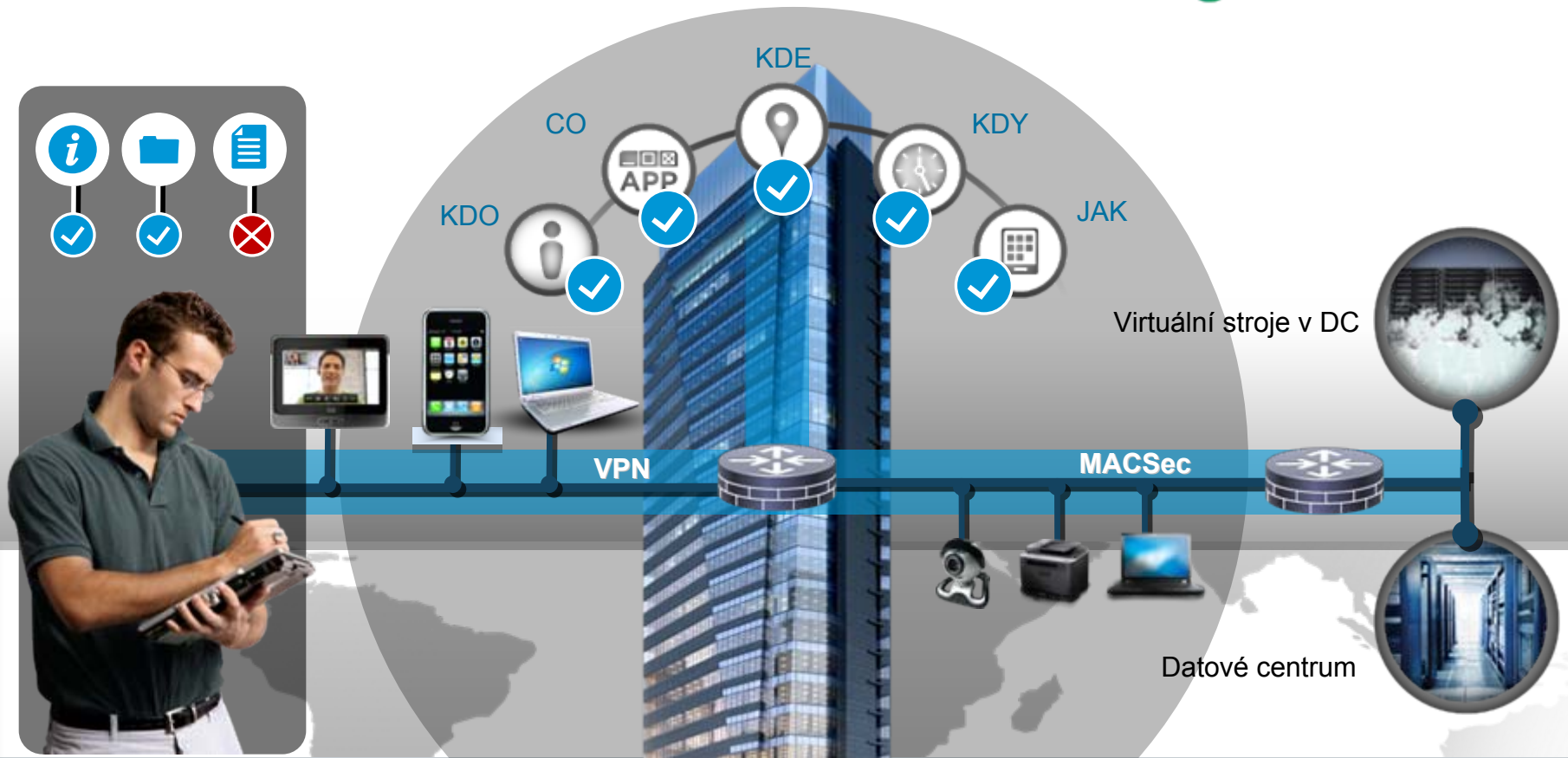
ÚLOHA

Přístup podle zařízení,
totožnosti a role
Přístup pro hosty

Prosazení pravidel od
koncového zařízení až po
datové centrum

Zajištění důvěrnosti
v celé síti

Cisco řešení: TrustSec technologie



CISCO ŘEŠENÍ

Konzistentní 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



Catalyst a Nexus přepínače, bezdrátová a směrovaná infrastruktura



Cisco ASA, ISR, ASR 1000

Prosazování
pravidel v koncových
zařízeních



NAC Agent

Trvalý i dočasný klient pro prohlídku a léčbu



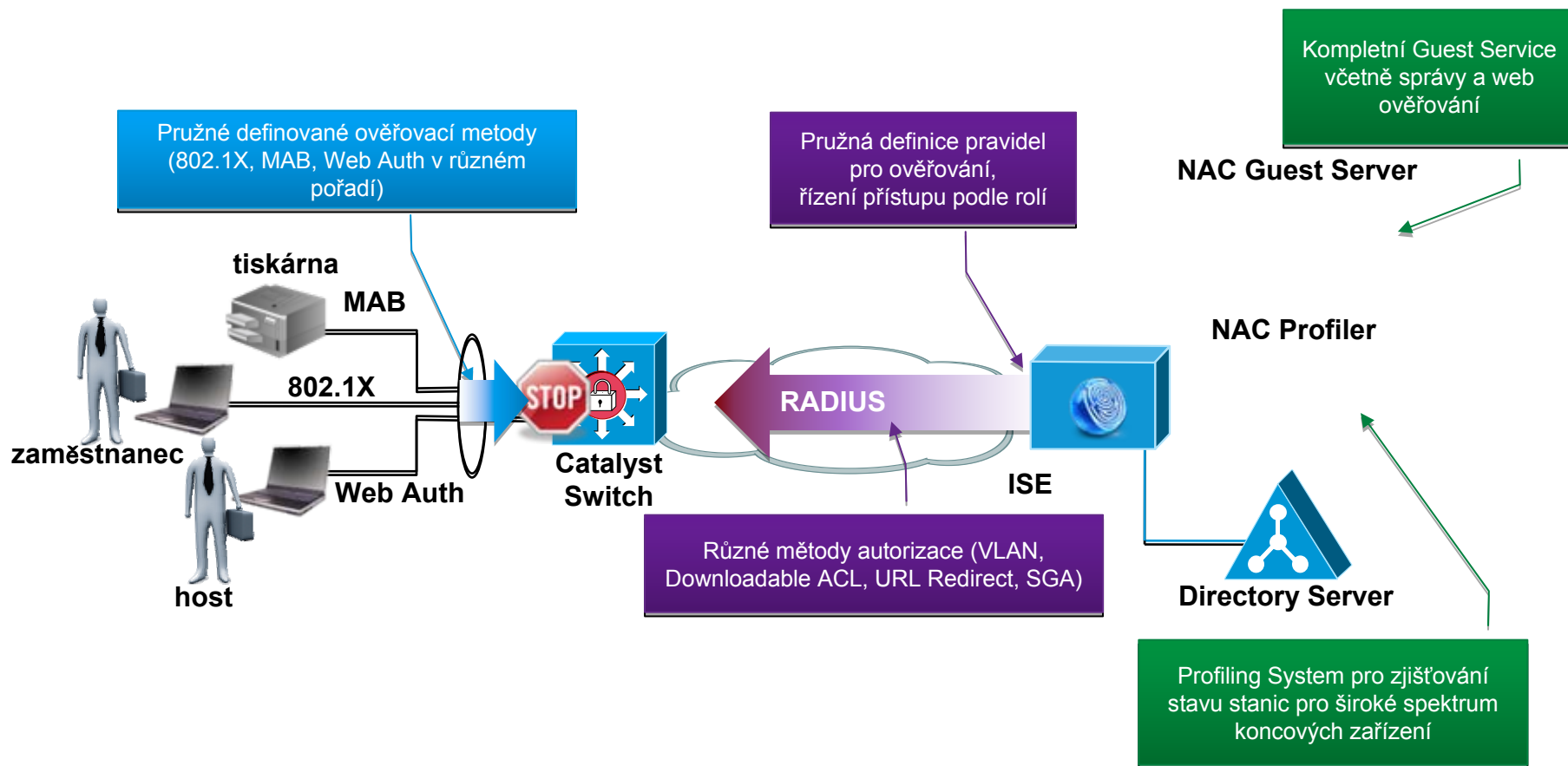
Web Agent



802.1x Supplicant

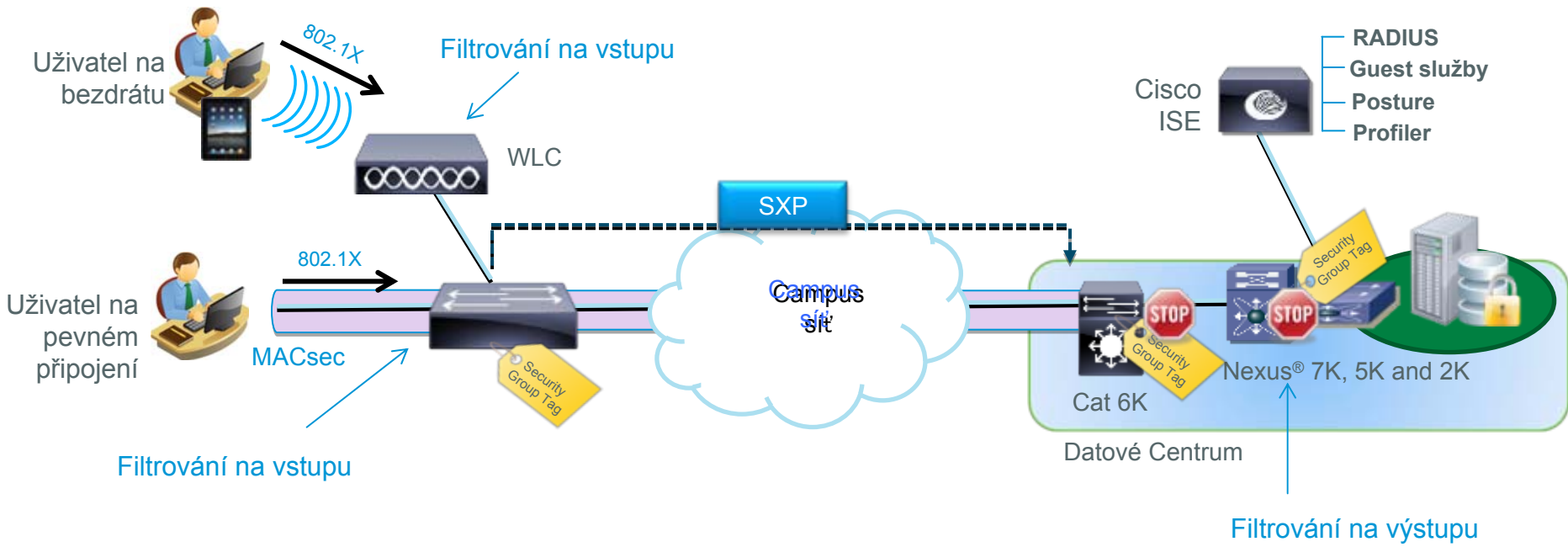
AnyConnect
OS-Embedded Supplicant

Trustsec řešení



TrustSec vlastnosti

Šifrování, SGT, SGA, SXP



Cisco inovace pro BYOD architekturu

Simplify IT Operations – Best of Breed – Best in Class

One Network (Predictability)

CleanAir

Chip level proactive and automatic interference mitigation

ClientLink

Chip level proactive and automatic electronic beamforming

Radio Resource Management

Automatic advanced RF shaping and management

VideoStream

Wired multicast efficiency over a Wireless network

TrustSec - Secure Group Access

Simplified user and resource based segmentation – independent of topology

Application Visibility & Control

Identify, analyze, and optimize application traffic

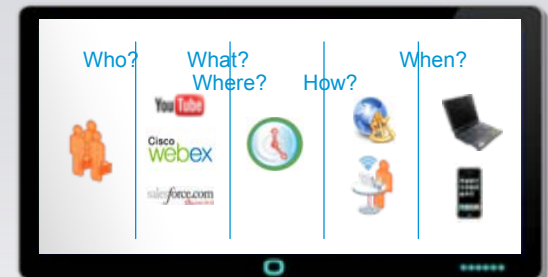
Stateful Switchover

Sub second WLAN & LAN convergence

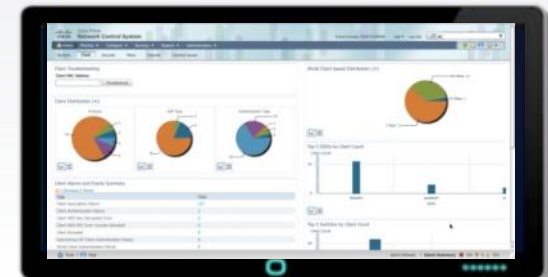
AnyConnect

Always-On context-aware VPN connectivity

One Policy & One Management



ISE
(Control)



Prime
(Visibility)

Novinka: Converged Access

Jednotná platforma pro pevné i bezdrátové řešení

WIRELESS

Features:

- 802.11n
- CleanAir
- VideoStream
- Radio Resource Management (RRM)
- Wireless Intrusion Prevention System (WiPS)
- 802.11ac Ready

WIRED

Features:

- Stacking
- Stackpower
- Trustsec/Identity
- AVC/Medianet
- Flexible Netflow
- Granular QoS
- Smart Operations
- EnergyWise

Benefits

- Built on **Doppler** – Cisco's Innovative Flexparser ASIC technology
- Eliminates operational complexity
- Single Operating System for wired and wireless

Note: All features may not be available on new platforms at introduction but are expected to be added within 12-18 months

BYOD 2.2: validovaný design

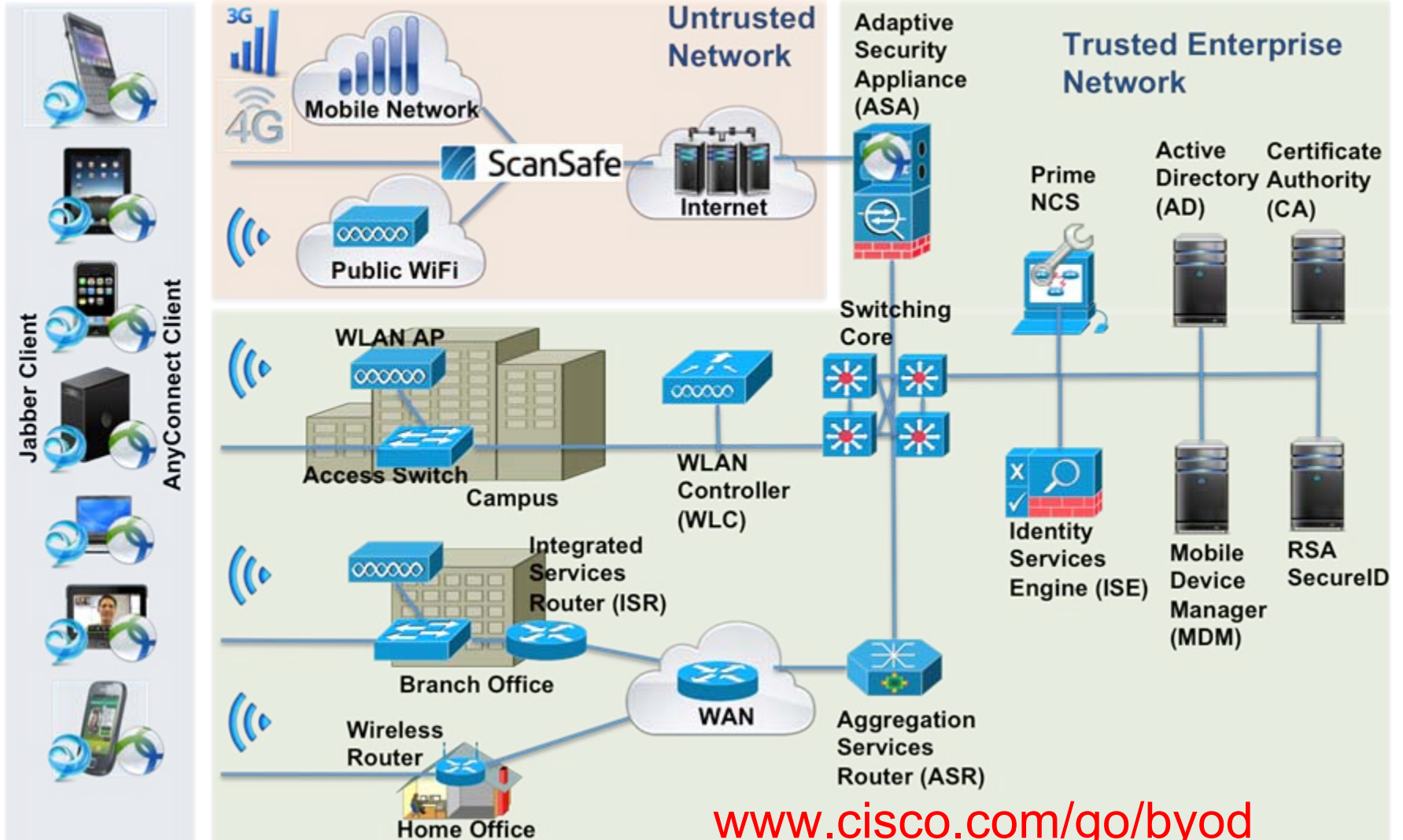
BYOD
Devices

Wired, Wireless,
Mobile Access

Access
Infrastructure

Off-Premise
Gateways

Security and Policy
Infrastructure



www.cisco.com/go/byod

www.cisco.com/go/byoddesign



Agenda

- Úvod
- Důsledky BYOD pro IT
- Cisco řešení pro BYOD
- Závěr

Závěr

Problematika **BYOD** existuje a je třeba ji řešit

BYOD přináší potřebu zásadních změn v IT pro každou organizaci

Cisco disponuje robustní architekturou a end-to-end škálou produktů pokrývající všechny nové nároky vyplývající z **BYOD** trendu

K dispozici jsou volně dostupné dokumenty Cisco Validated Designs (CVD) popisující komplexní ověřené funkční řešení **BYOD**

Děkujeme



www.cisco.com/go/byod

www.cisco.com/go/byoddesign



Agenda

- Úvod
- Důsledky BYOD pro IT
- **Způsoby nasazení BYOD**
- Cisco řešení pro BYOD
- Závěr

Typické způsoby nasazení BYOD



Omezující

Základní

Rozšířené

Pokročilé

Prostředí vyžadující
přísnou kontrolu

Pouze firemní zařízení
Výroba
Citlivé obchodování
Klasifikované sítě státní
správy
Tradiční podniky

Základní služby a
jednoduchý přístup

Více typů zařízení,
pouze internet
Vzdělávací instituce
Veřejné instituce
Jednoduchý přístup pro
hosty

Různorodé aplikace,
bezpečná aktivace služeb

Více typů zařízení a
přístupových metod, VDI
Zdravotnictví
Podniky se zájmem o BYOD
Podpora kontraktorů

Široká podpora aplikací,
nové služby, plná kontrola

Více typů zařízení MDM
Inovativní firmy
Retail on Demand
Podpora mobilního prodeje
(Video, Collaboration, etc.)

Stavební kameny řešení BYOD

Pokročilé

Collaboration aplikace

WebEx, Jabber

Správa pracovního prostředí

MDM

Rozšířené

Bezpečná mobilita

AnyConnect, ASA,
ScanSafe, WSA

Omezující
a základní

Správa pravidel v
infrastruktuře

ISE

Síťová infrastruktura

Správa pevných
i bezdrátových sítí
Prime