

Bezpečnost sítí

6. 4. 2017

Jiří Žiška



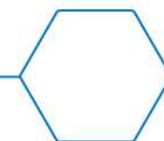
Proč řešit bezpečnost?

- Dle statistik je až 90% všech útoků provedeno zevnitř sítě
- Zodpovědnost za útoky z vaší sítě má vždy provozovatel
- Bezpečnost je jen jedna pro bezdrátovou i drátovou síť

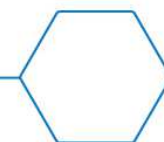


Kde řešit bezpečnost?

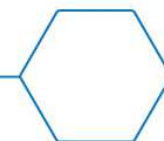
- > U bezdrátových sítí
- > U drátových sítí
- > Na routerech
- > Ve VPN
- > Na aplikační úrovni
- > Správa aktivních prvků



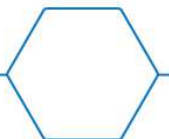
- Šifrování a autentizace jsou téměř nezávislé
- Šifrování se používá především ve WiFi
- Typy šifrování WiFi
 - WEP
 - WPA-TKIP
 - **IEEE 802.11i (WPA2-AES)**



- Otevřená síť
- MAC adresa
- Web portal
- Jednotné heslo (pouze WiFi)
- IEEE 802.1X
 - Jménem a heslem
 - Pomocí certifikátů a SmartCard

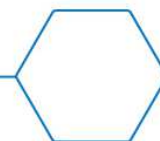


- Vydání 2001 (2004, 2010)
- Původně určen pro porty na drátové síti
- Nutný klient (supplicant) na zařízení, které se přihlašuje do sítě
- Ve výchozím nastavení neumožňuje přístup do sítě zařízením bez supplicantu

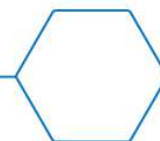


Flex-auth Sequencing

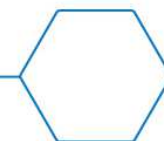
- Umožňuje se do zabezpečené sítě přihlásit i bez 802.1X supplicantu
- Podporováno na Cisco přepínačích i u některých jiných výrobců
- V bezdrátových sítích je omezené



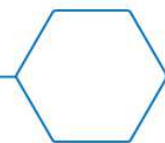
Cisco Identity Services Engine



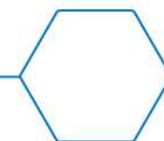
- HW i Virtuální platforma
- Podpora VMware, Hyper-V i KVM
- Různé licence
- Možnost HA
- Standalone nebo distribuovaná architektura



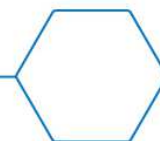
- Podpora velkého množství databází
- Mnohem více než jen RADIUS
- Předdefinované profily pro různé výrobce (nejen Cisco)
- Možnost propojení s Cisco Prime Infrastructure
- API



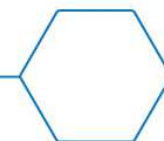
- Guest Portal
- RADIUS
- TACACS+
- VPN
- Klasifikace koncových zařízení
- BYOD
- Posture



- Autentizace na základě polohy
- Podpora MDM
- Portál pro generování certifikátů
- TrustSec
- pxGrid
- Easy Connect (PassiveID)



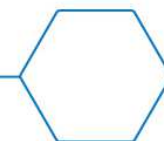
- Standalone architektura
 - Možnost HA
- Distribuovaná architektura
- Podpora od jednotek klientů až po stovky tisíc klientů



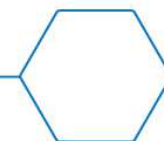
- Interní databáze (pro uživatele i koncová zařízení)
- Active Directory
 - Možnost více domén
 - Trusted domény
- LDAP (RFC 2251)
- RADIUS Token identity source (RFC 2865) a RSA RADIUS token server
- Certificate authentication profile



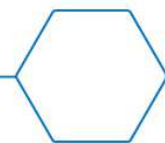
- Možnost vytvoření vlastního vzhledu portálu (plná customizace)
- 15 předdefinovaných jazyků
- Možnost vytváření portálu ve WYSIWYG editoru (isepb.cisco.com)
- Uživatelské účty mohou vytvářet vybraní zaměstnanci
 - Účty lze vytvářet pro jednotlivce i hromadně
 - Lze omezit vytváření účtů dle skupin
 - Lze definovat, kdo účty může spravovat



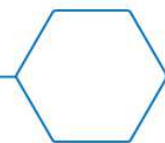
- Účet si může vytvořit sám uživatel (self-registration)
 - Vytváření účtů lze omezit pomocí PIN kódu
 - Vytvořené účty mohou vyžadovat schválení navštívenou osobou nebo pověřeným zaměstnancem
- Účty lze předat různými způsoby
 - Tisk
 - E-mail
 - SMS



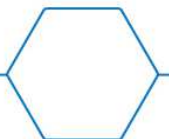
- Platnost lze nastavit od prvního přihlášení
- Možnost zobrazení reklamy
- Lze propojit s registračním portálem zařízení zaměstnanců
- Portálů může být více (např. dle polohy)



- RADIUS pro Autentizaci, Autorizaci a Accounting (zaznamenávání)
- Možnost ověřit a definovat práva pro přístup na síťové aktivní prvky (TACACS+)
- Podpora mnoha protokolů (např. MS-ChapV2, EAP-GTC, PEAP, EAP-TLS, PEAP-TLS, EAP-FAST)
- Proxy funkce pro externí RADIUS (např. EDUROAM)
- Lze volit pořadí databází, u kterých se uživatel ověřuje

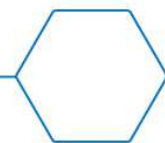


- Lze aplikovat VLAN nebo filtr (ACL) dle:
 - Uživatele (Role, skupiny)
 - Stavů a typu koncového zařízení (Profiling)
 - Místa připojení
 - Historie připojení
- Politiky lze měnit „za běhu“ pomocí CoA (RFC 3576)

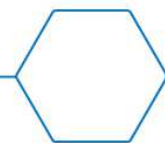


ISE – AAA (Accounting)

- Zaznamenávání aktivity uživatelů a zařízení připojených v síti
- Systém pro sledování výstrah (úspěšná/neúspěšná přihlašování, neaktivita, stav systému AAA, dostupnost externích databází, aktivita filtrů)



- Automatické rozpoznávání a klasifikace připojených zařízení
- Předdefinované profily pro běžná mobilní zařízení
- Předdefinované profily pro síťová zařízení (NAD) různých výrobců
- Podpora pro IPv6



- Co si představit pod pojmem BYOD???
- Registrace a provisioning klientských zařízení
- Specifické podmínky pro BYOD zařízení
- Možnost vydávání certifikátů pro BYOD zařízení
- Možnost automatické konfigurace BYOD zařízení (Windows, MacOS, iOS, android)

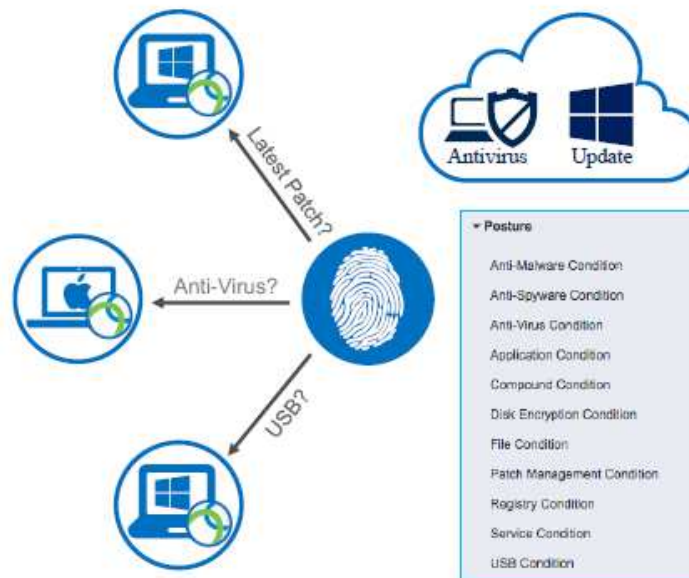


Posture assessment

Posture defines the state of compliance with the company's security policy

Posture Flow

- 
AUTHENTICATE USER/DEVICE
 Posture: Unknown / Non-Compliant ?
- 
QUARANTINE
 Limited Access: VLAN / dACL / SGTs
- 
POSTURE ASSESMENT
 Check Hotfix, AV, Pin lock, USB Device, etc.
- 
REMEDIATION
 WSUS, Launch App, Scripts, MDM, etc.
- 
AUTHORIZATION CHANGE
 Full Access – VLAN / dACL / SGTs.



148

3rd Party EMM Vendor Support – APIv1

CITRIX®
XenMobile
Version 7.1

 **MobileIron**
Version 5.5

SOTI®
SOTI MobiControl 12.4

 **Good**
POWERED BY BLACKBERRY
Version 2.3

 **GLOBO™**
GO!Enterprise MDM v3.7

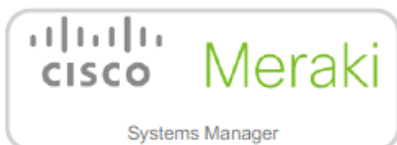
 **Symantec™**
App Center v4.1.10

MaaS360®
by Fiberlink, an IBM company
Cisco MCMS v1.0 

ABSOLUTE™
Data & Device Security


Version 13.2 Patch 5

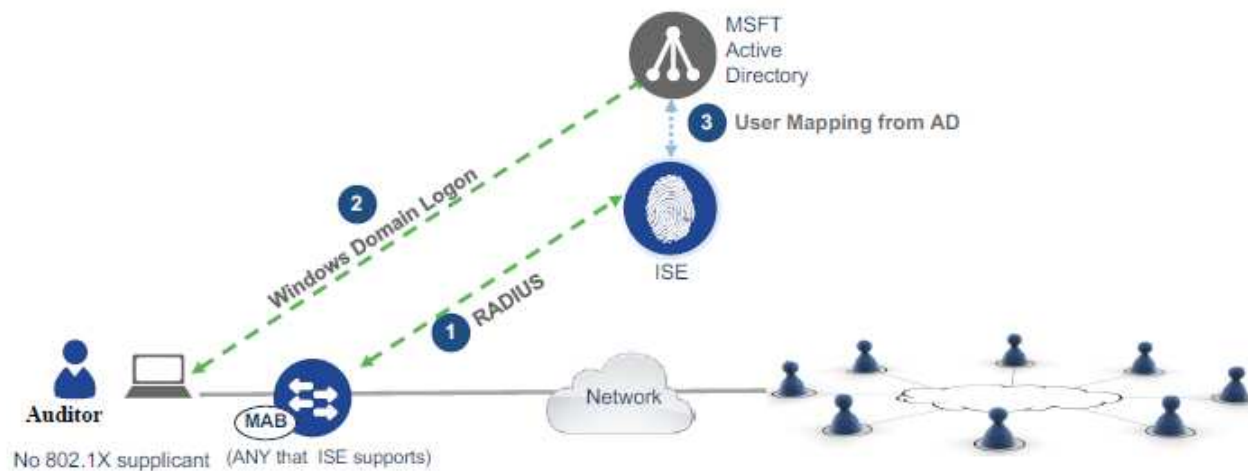
3rd Party EMM Vendor Support – APIv2



Cisco ISE MDM APIv2 is fully backward compatible with APIv1

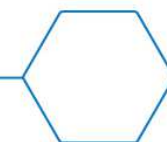
(*) Subject of change w/o further notification

ISE – Easy Connect



ISE – Vendor compatibility

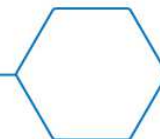
Device Type	Vendor	CoA Type	URL Redirect Type	Supported/Validated Use Cases				
				802.1X/MAB	Profiler without CoA	Profiler with CoA	Posture	Guest/BYOD
Wireless	Aruba 7000, InstantAP	RADIUS	Static URL	√	√	√	√	√
	Motorola RFS 4000	RADIUS	Dynamic URL	√	√	√	√	√
	HP 830	RADIUS	Static URL	√	√	√	√	√
	Ruckus ZD 1200	RADIUS	–	√	√	√	–	–



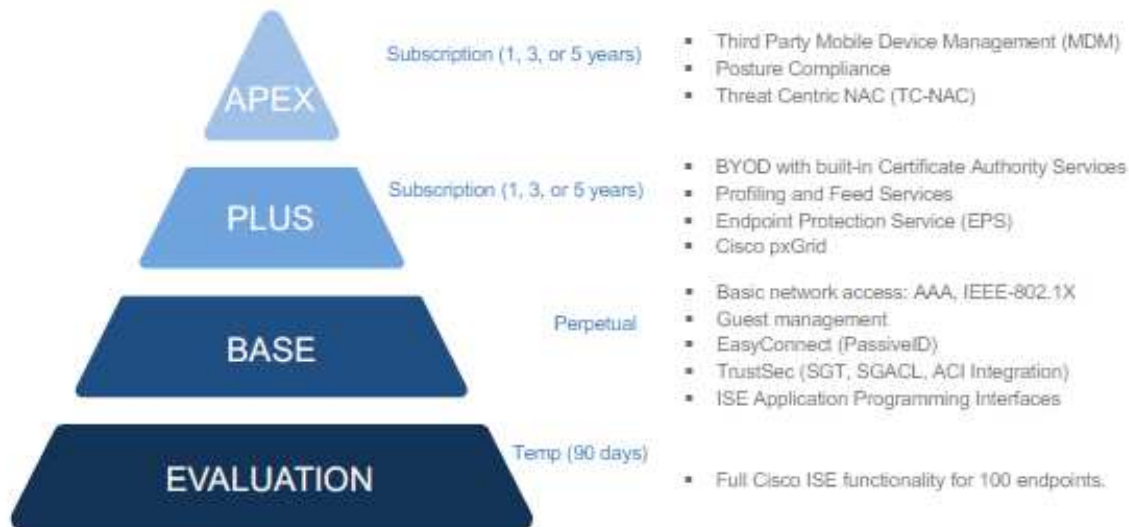
ISE – Vendor compatibility

Device Type	Vendor	CoA Type	URL Redirect Type	Supported/Validated Use Cases				
				802.1X/MAB	Profiler without CoA	Profiler with CoA	Posture	Guest/BYOD
Wired	HP A5500	RADIUS	Auth VLAN provided by ISE	√	√	√	√	√
	HP 3800 and 2920 (ProCurve)	RADIUS	Auth VLAN provided by ISE	√	√	√	√	√
	Alcatel 6850	SNMP	Dynamic URL	√	√	√	√	√
	Brocade ICX 6610	RADIUS	Auth VLAN provided by ISE	√	√	√	√	√
	Juniper EX3300-24p	RADIUS	Auth VLAN provided by ISE	√	√	√	√	√
For additional third-party NADs, you must identify the device properties and capabilities and create custom NAD profiles in Cisco ISE.				√	√	Requires CoA support	Requires CoA support. For URL redirect, if the wired device has no URL redirect, utilizes ISE Auth VLAN. Wireless devices have not been tested with Auth VLAN.	

- Každý node je HW nebo virtual appliance
 - Virtual appliance není zdarma
 - Support se kupuje pouze pro HW nebo virtual appliance
- Existují 3 typy licencí BASE, PLUS a APEX
- Zvlášť licence pro TACACS+



- Licenses are uploaded to the Primary Administration node and propagated to the other Cisco ISE nodes in the cluster
- Base license is fundamental for use of Plus / Apex services.



ADDITIONAL OPTIONS

DEVICE ADMIN

Perpetual

- Cisco ISE requires a Device Administration license to use the TACACS+ service on top of an existing Base license.



ISE – Express Bundle

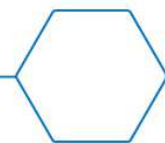
- Standalone verze ISE
- Lze pouze jeden virtuální stroj
- Nelze použít HA (pouze na úrovni virtualizace)
- Součástí licence pro 150 zařízení
- Lze licencovat pomocí BASE, PLUS i APEX licencí až do 5000 zařízení
- Nelze použít s TACACS+ licencí
- Velmi výhodná cena

ISE – Upgrade ACS

- Brzy bude vyhlášeno End-Of-Sale ACS 5.8
- Lze upgradovat z ACS na ISE za zvýhodněných podmínek
- Možnost upgrade s EoS pravděpodobně také skončí
- Upgrade lze provést od verze 5.5 výše



- MAC adresy jsou nedostatečné zabezpečení (zejména chybí šifrování v bezdrátových sítích)
- ISE slouží k přihlášení a přidělení práv hostům a zaměstnancům (na firemních i soukromých zařízeních)
- Síla ISE je zejména v komplexnosti řešení a integraci s ostatními systémy
- Zabezpečení lze kombinovat a řešit kontext
- Lze sjednotit bezpečnost pro uživatele v bezdrátové, drátové i VPN síti



> Děkuji za pozornost.

UNIS COMPUTERS, a.s.

Jundrovská 31, 624 00 Brno

tel.: +420 544 528 301

fax: +420 541 223 134

obchod@uniscomp.cz

Pobočka Praha

Zelený pruh 95/97, 140 00 Praha 4

tel.: +420 227 230 080

■ www.uniscomp.cz