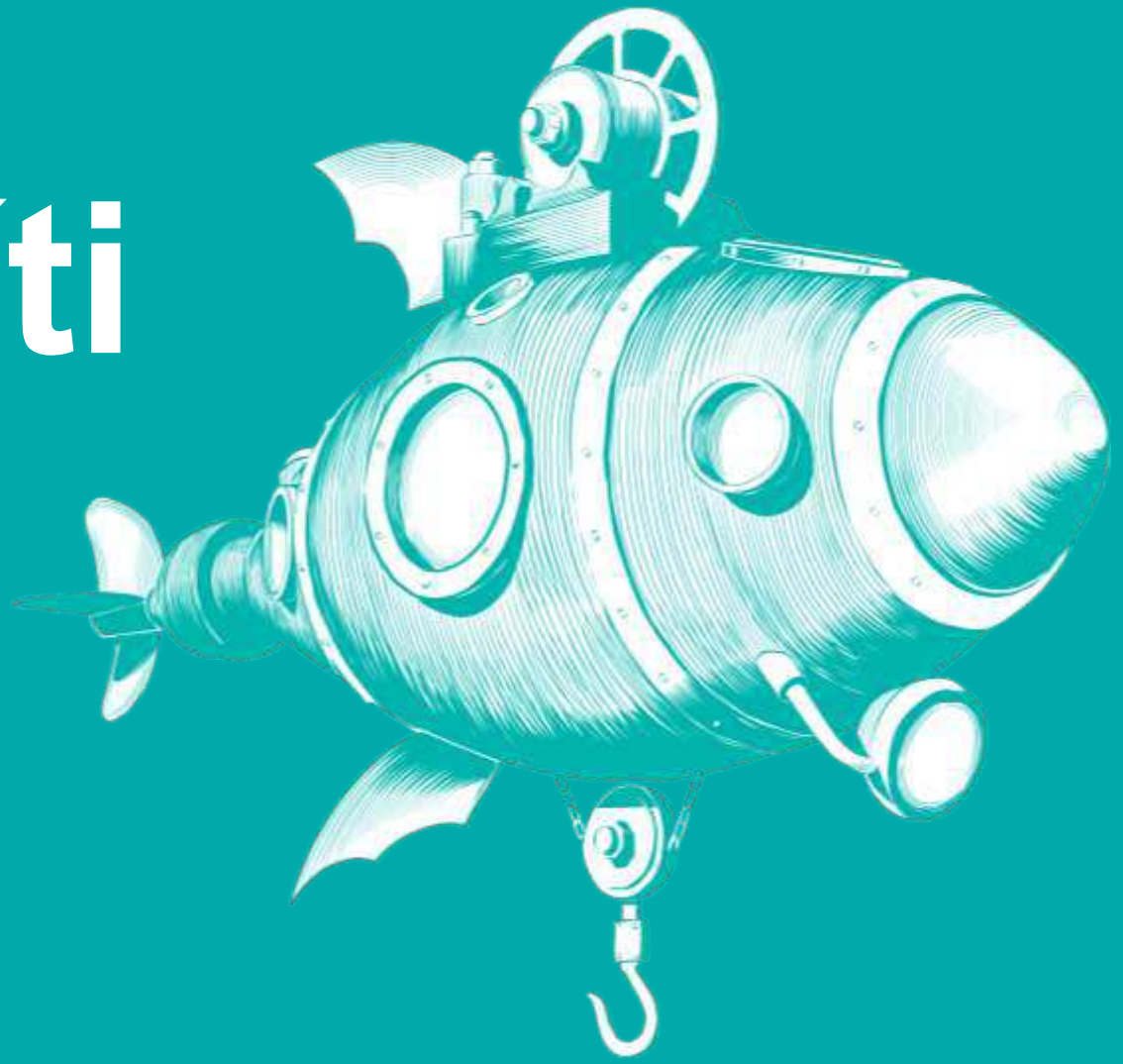
ALEF

CISCO Partner

Identita v síti

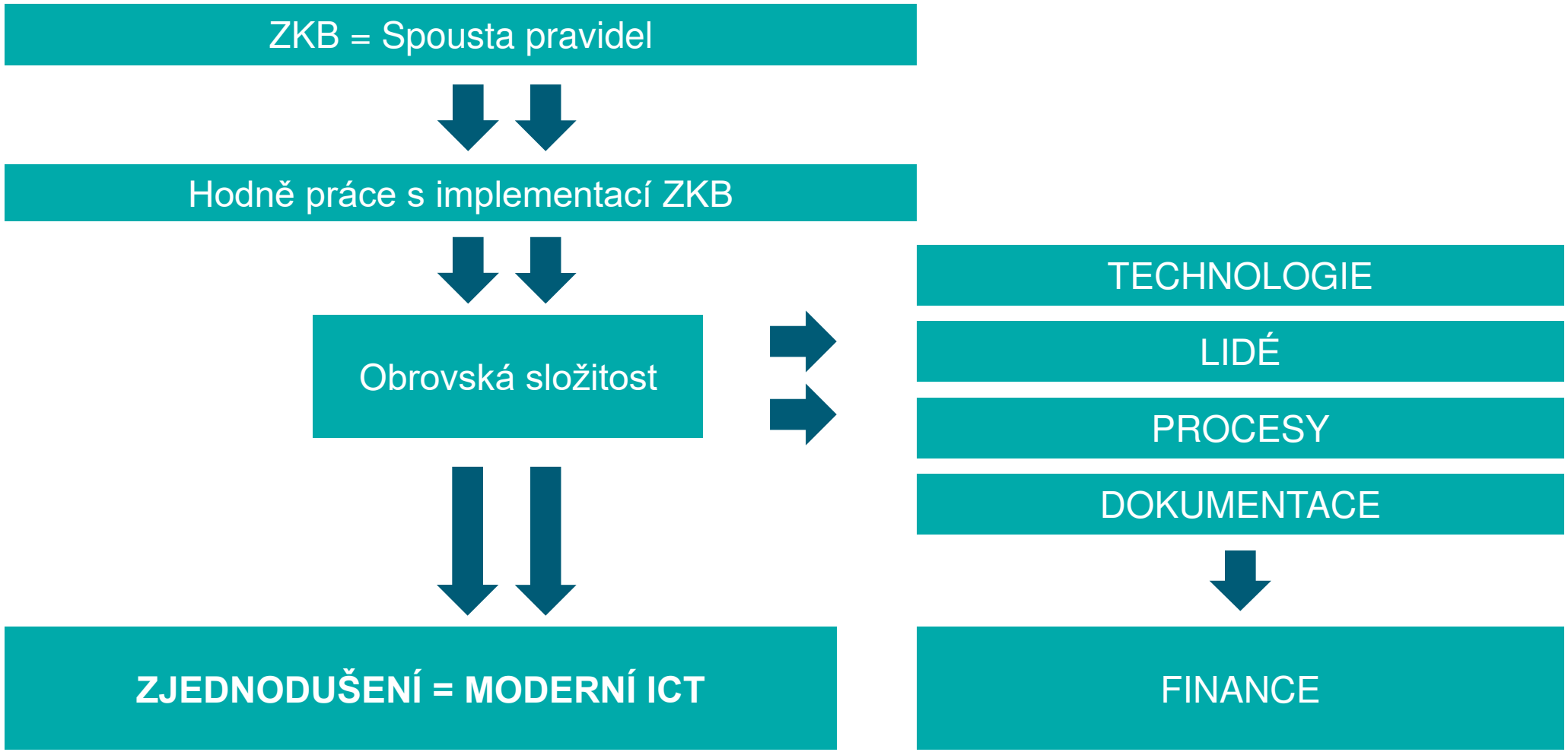
(Moderní využití identity v sítích)



Jiří Herzig

Consultant, Security

ALEF Nula a.s.

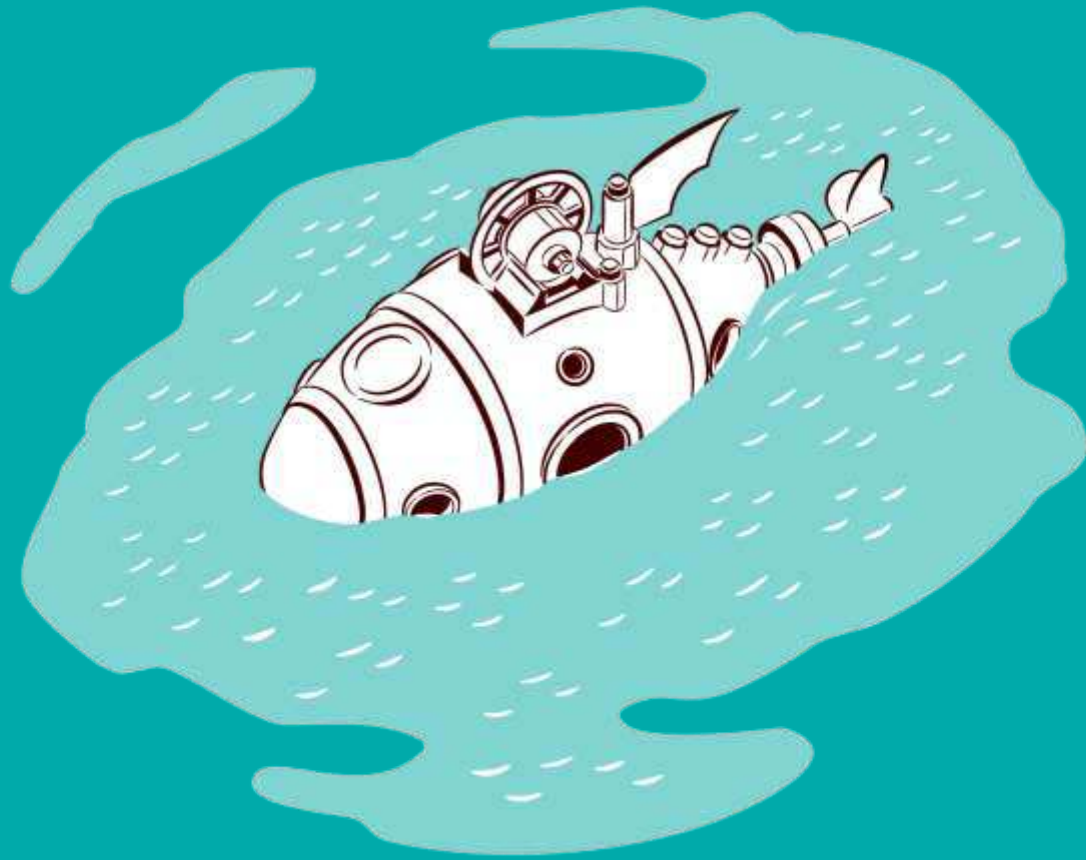

ZKB = Spousta pravidel
Hodně práce s implementací ZKB
Obrovská složitost
ZJEDNODUŠENÍ = MODERNÍ ICT
TECHNOLOGIE
LIDÉ
PROCESY
DOKUMENTACE
FINANCE

ALEF

ALEF

CISCO Partner

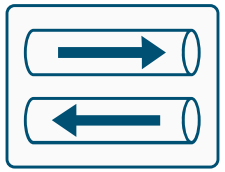
Motivace pro práci s identitou



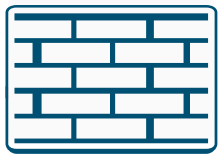
Proč chceme využívat identitu?

Web proxy

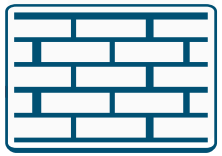
VPN koncentrátor



Interní FW



Datacenter FW



ISE (NAC)

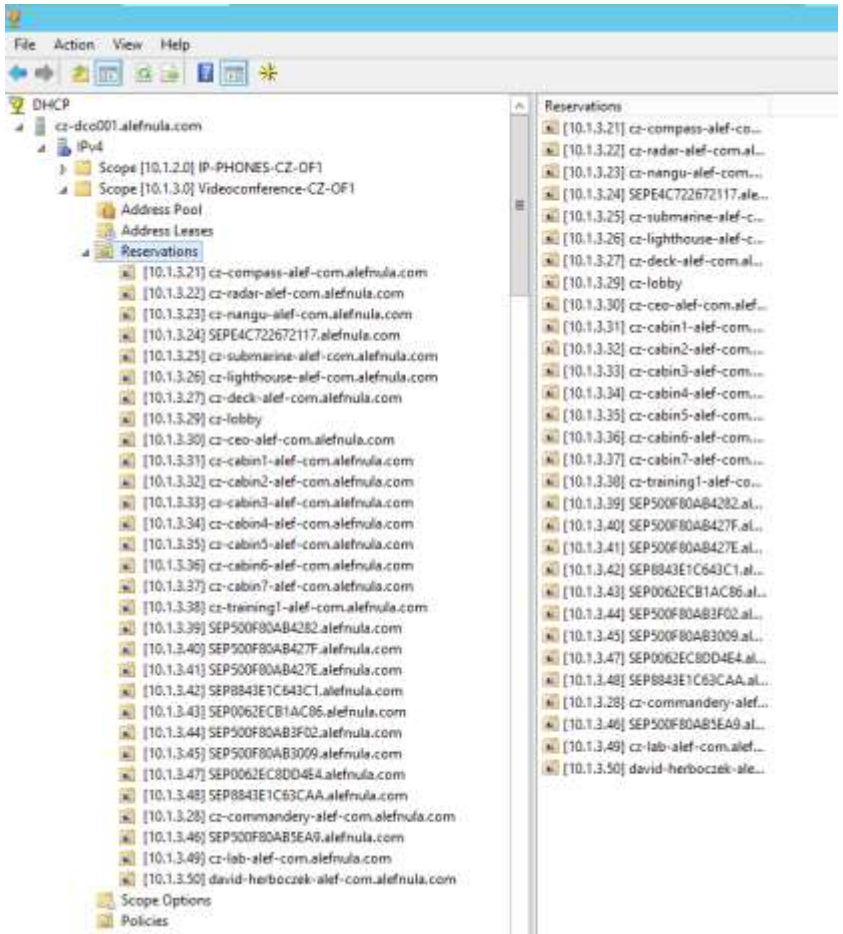
Stealthwatch

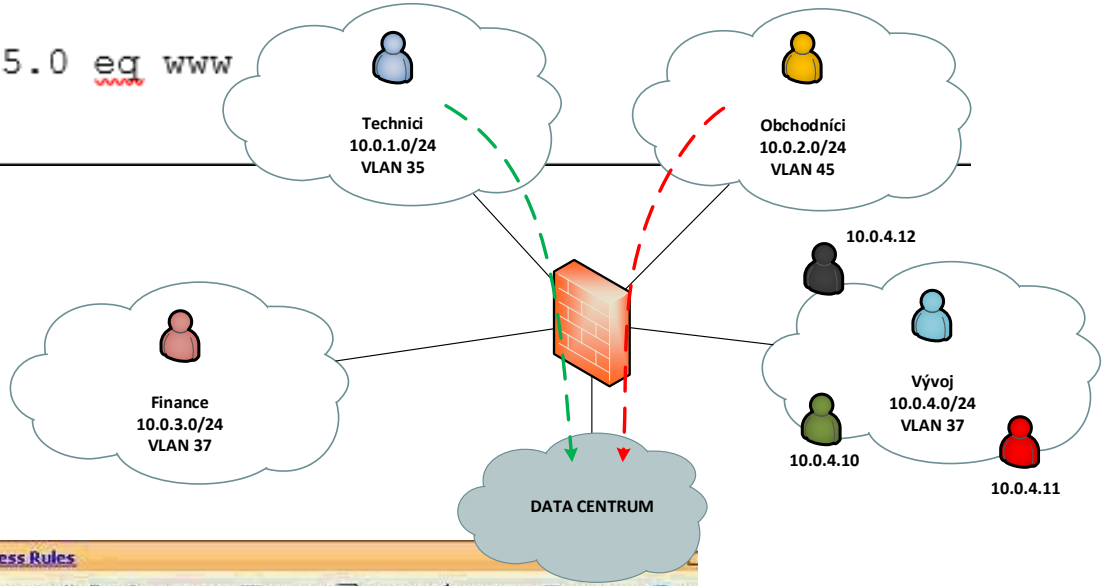
Proč chceme využívat identitu?

```
permit tcp host 10.0.0.1 any host 192.168.1.1 eq ssh

permit tcp 10.0.0.0 255.255.255.0 any 192.168.1.0 255.255.255.0 eq www

permit icmp 10.100.0.0 255.255.255.0 any
```

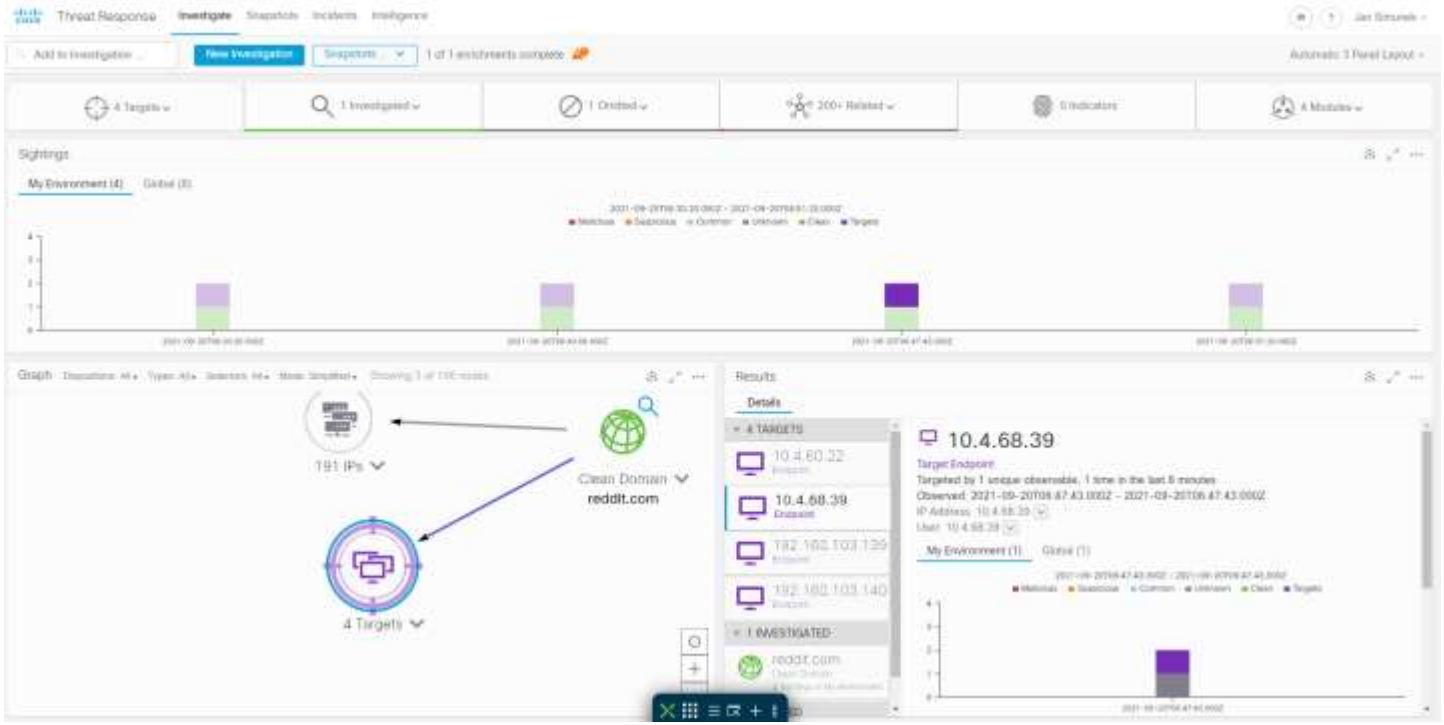




ALEF

Proč chceme využívat identitu?

Flow information	Packets
Source address	10.1.8.3
Destination address	172.168.134.2
Source port	47321
Destination port	443
Interface	Gi0/0/1
IP TOS	0x00
IP protocol	6
Next hop	172.168.25.1
TCP flags	0x1A
Source SGT	100
:	:
ETA meta data	IDP | SPLT
Application name	NBAR SECURE-HTTP



Request	Destination	Internal IP	External IP	Action	Categories	Application
DNS	ws.amateri.com	10.80.14.14		Blocked	**Pornography,** Adult Themes	
DNS	chrome.cloudflare-dns.com		:28d0::46	Blocked	**Application Block,** Proxy/Anonymizer	1.1.1.1 App
DNS	chrome.cloudflare-dns.com		:28d0::46	Blocked	**Application Block,** Proxy/Anonymizer	1.1.1.1 App

ALEF

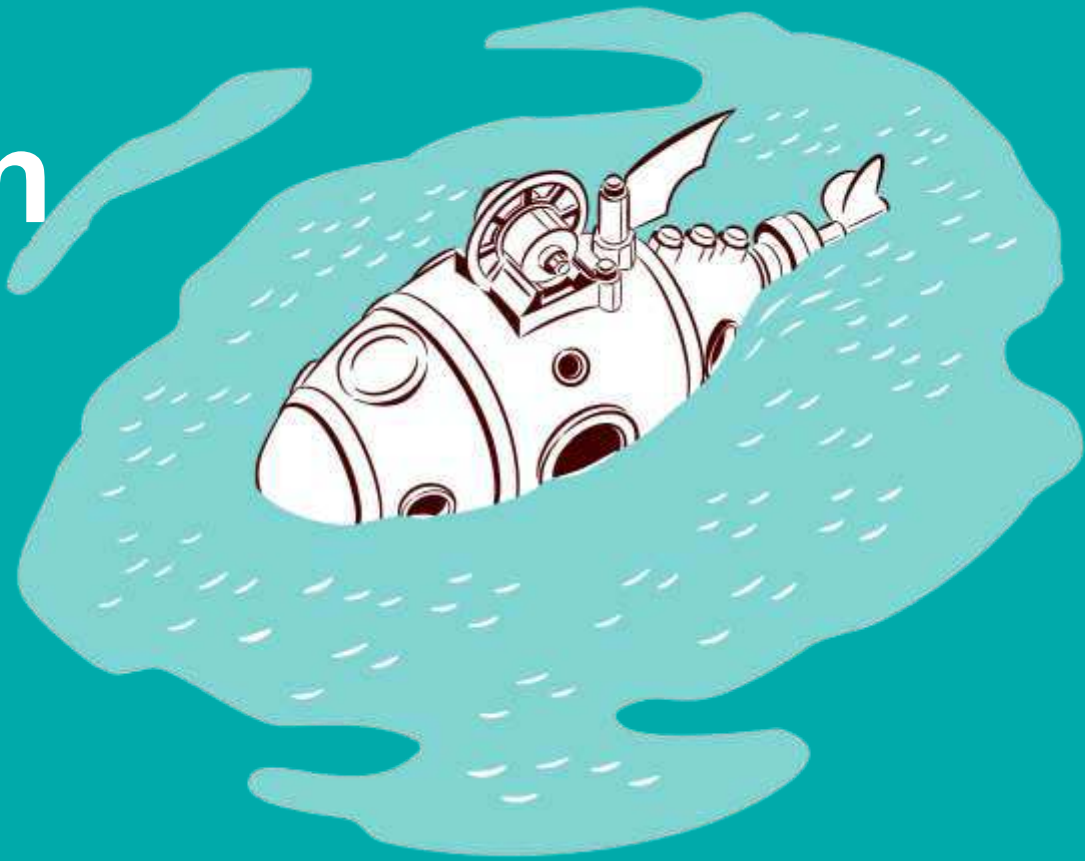
Nevýhody realizací bez identitního přístupu

- Velké množství DHCP rezervací pro výjimky.
- Velká složitost bezpečnostních pravidel.
- Obrovská zátěž na IT zaměstnance.
- Malá škálovatelnost řešení ve vazbě na růst prostředí Zákazníka.
- Vysoká složitost HR a IT interních procesů.

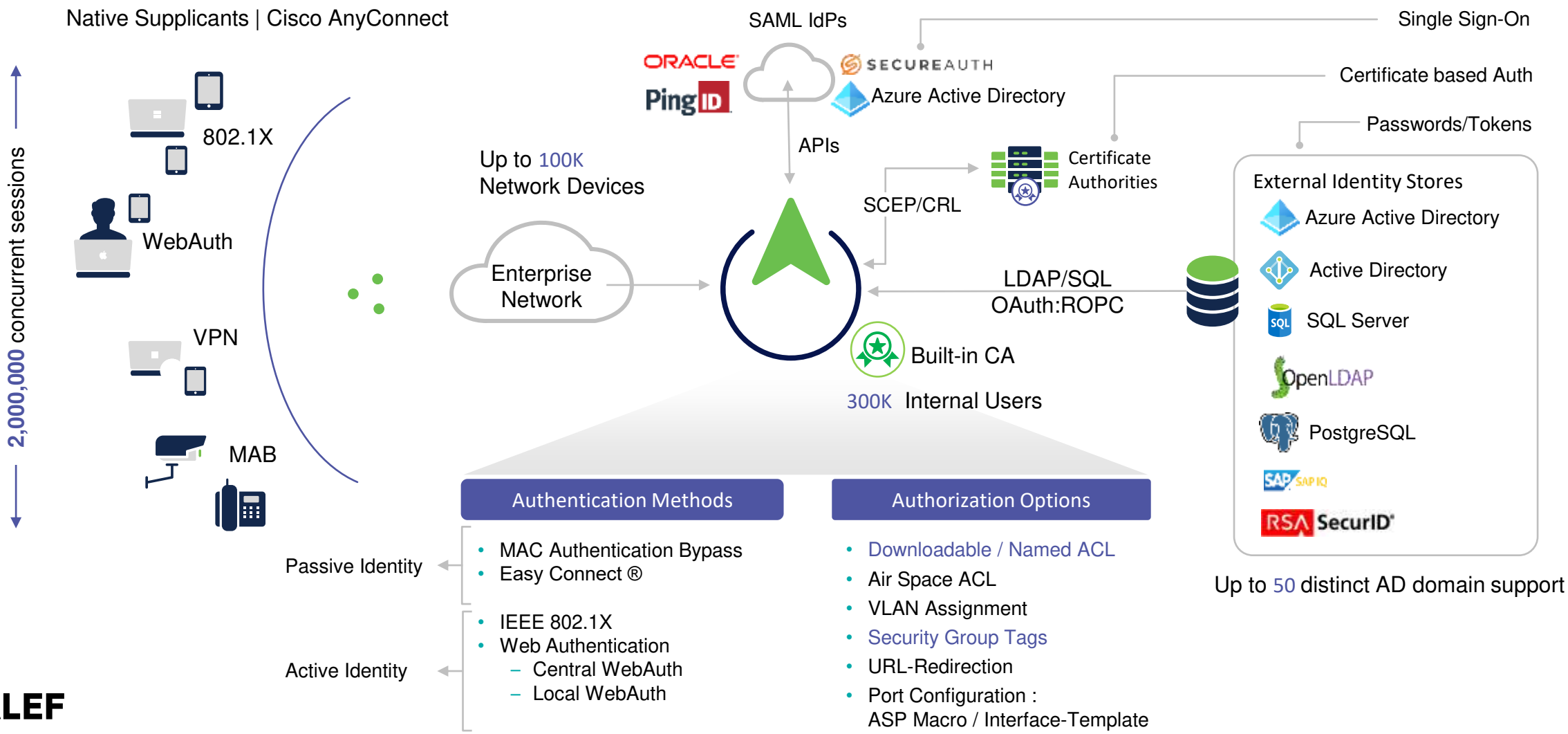
ALEF

CISCO Partner

Identita v moderních sítích

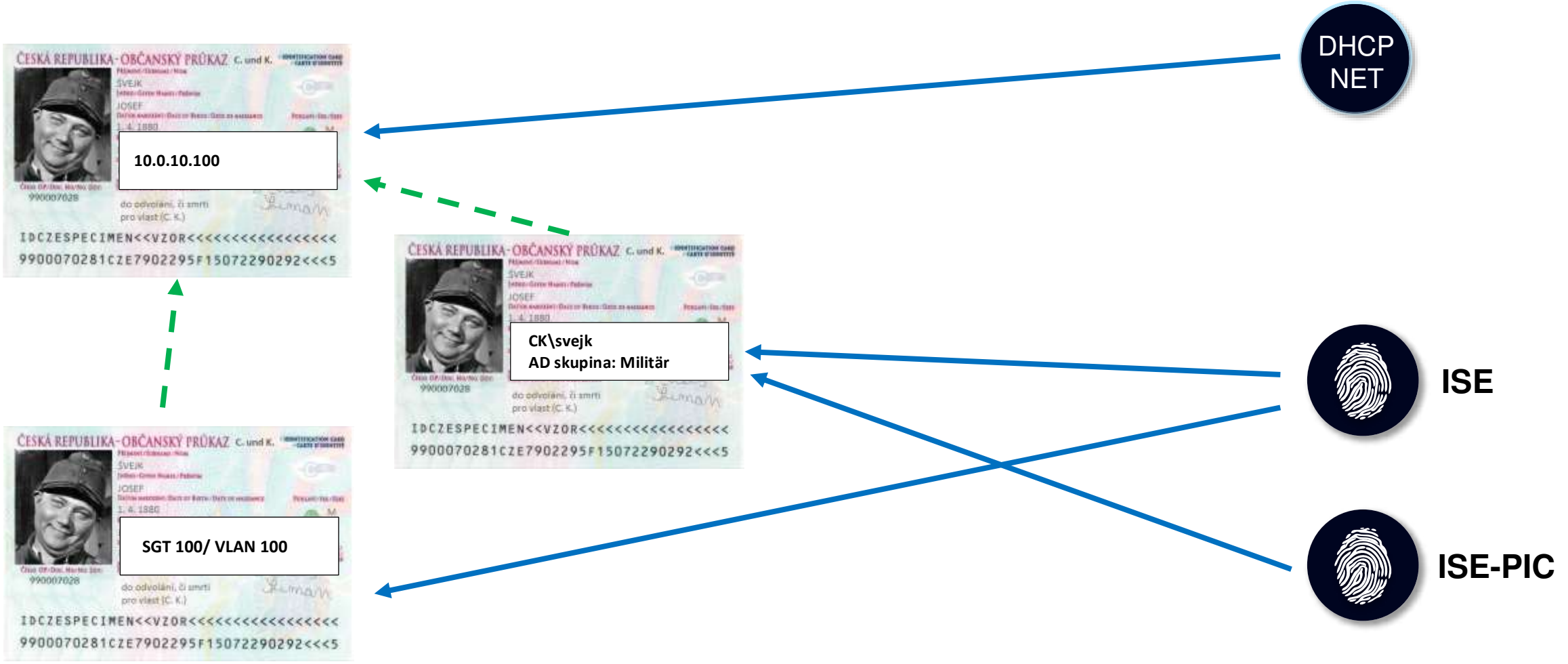


Identity Services Engine



ALEF

Identita a jak ji získat?

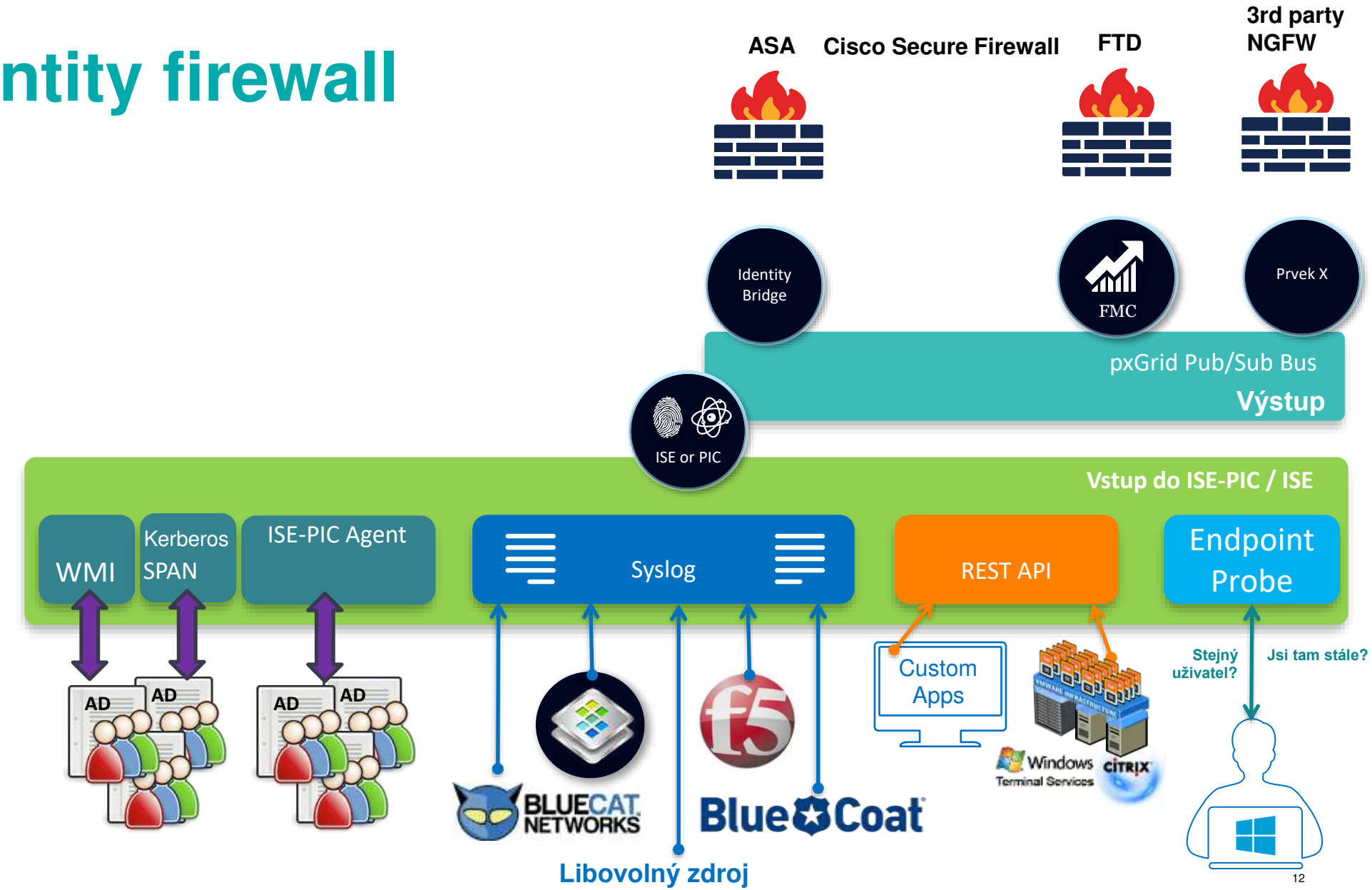


ALEF

Cisco ISE (online centralizace IP:username)

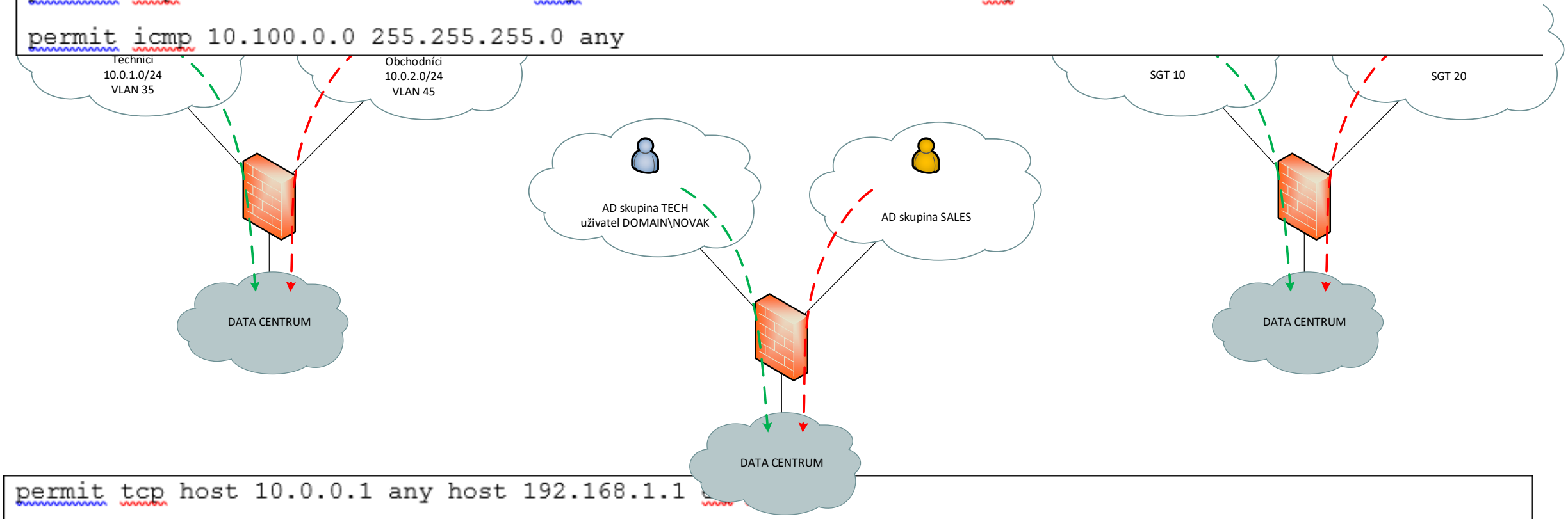
MAC Address	IPv4 Address	Username	Hostname	Endpoint Profile
MAC Address	IPv4 Address	Username	Hostname	Endpoint Profile
00:22:BD:D3:5B:2F	10.34.75.13			Cisco-IP-Camera
00:02:4B:CC:D6:63	10.35.68.203			Cisco-IP-Phone
5C:F9:38:AA:1F:90	10.32.2.127	jim	Jim-Air	Apple-MacBook
30:46:9A:2E:C3:F0	10.86.98.138	host/ALICE	win7pc	Microsoft-Workstation

Identity firewall



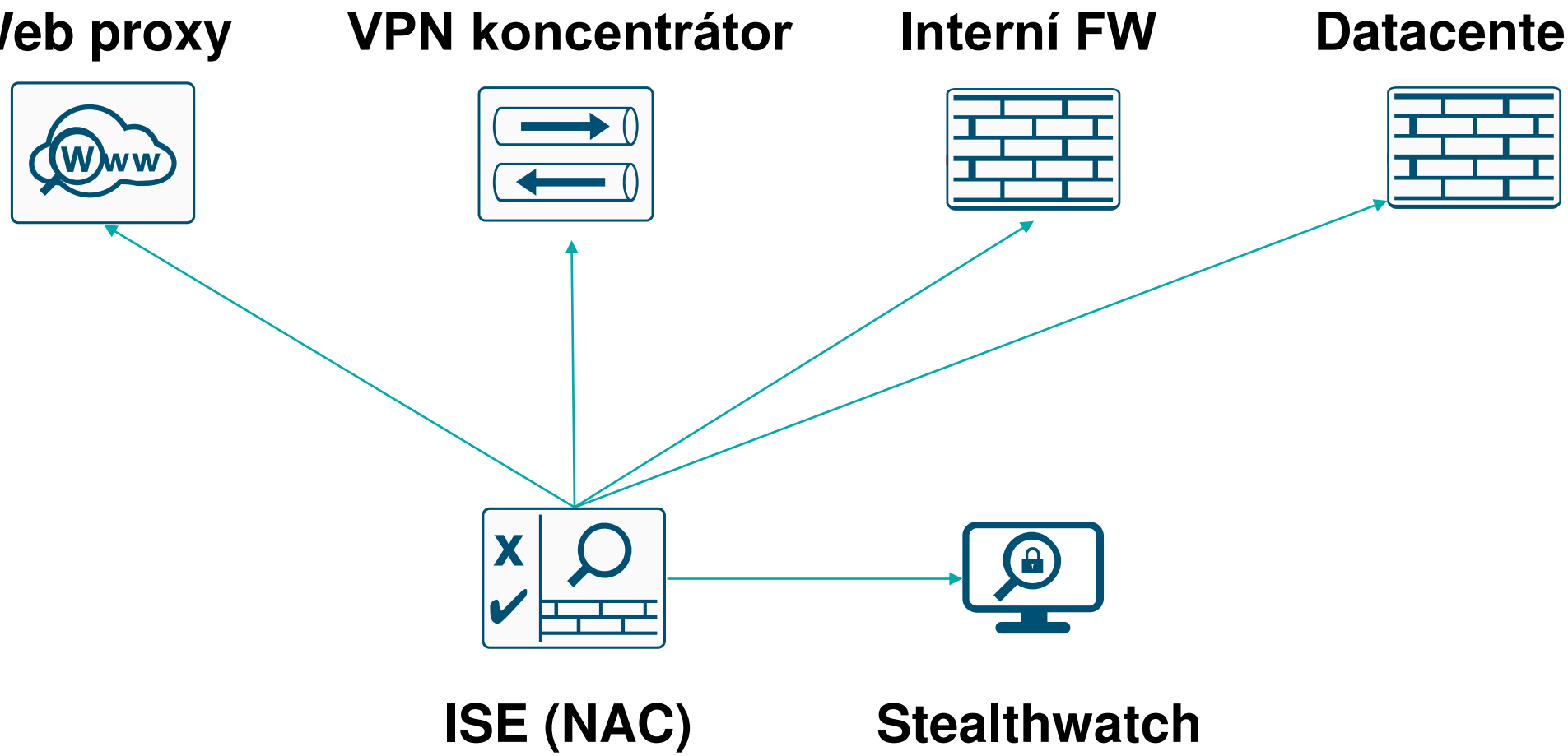
ALEF

```
permit tcp host 10.0.0.1 any host 192.168.1.1 eq ssh
permit tcp 10.0.0.0 255.255.255.0 any 192.168.1.0 255.255.255.0 eq www
permit icmp 10.100.0.0 255.255.255.0 any
```




```
permit tcp host 10.0.0.1 any host 192.168.1.1
permit tcp 10.0.0.0 255.255.255.0 any 192.168.1.0 255.255.255.0 eq www
permit icmp 10.100.0.0 255.255.255.0 any
permit ip user DOMAIN\JNOVAK object-group net-dc security-group name SGT_SAP_PREZ any
permit ip user-group DOMAIN\\TECH-USERS object-group net-dc security-group name SGT_OUTLOOK any
permit sctp user-group DOMAIN\\TECH-USERS any security-group name SGT_MGMT_NET any eq ssh
```

Více než jen Identity firewall

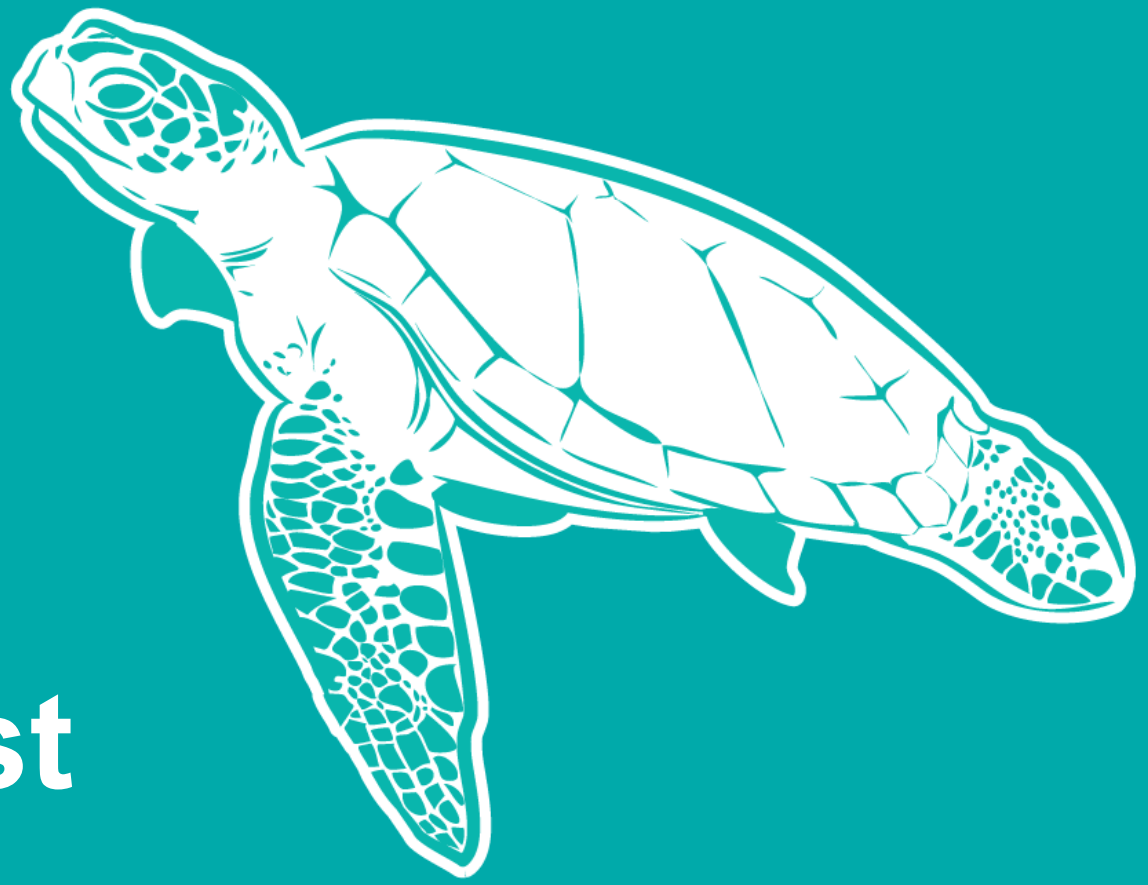


Výhody využití identity v síti

- Zajištění bezpečného přístupu uživatelů mezi segmenty a do datacentra.
- Zjednodušení bezpečnostních pravidel
  - eliminace vazby statické IP adresy či dedikovaného segmentu na uživ.
- Snížení komplexity systému uživatelských VLAN.
- Eliminace bezpečnostních rizik.
- Rychlejší incident response a přehlednost pravidel.
- Zajištění souladu s požadavky regulátora, odstranění auditních nálezů.

ALEF

CISCO Partner



Děkuji za pozornost