The bridge to possible

iDEME Bratislava ‘22
Informatizácia až po dediny a mestá

Bezpečný prístup k dátam a službám na základe identity

Milan Rášo, Systems Engineer, Cisco Slovensko

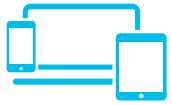
22.06.2022

Posun v IT prostredí

Používatelia, zariadenia a aplikácie odkiaľkoľvek

VPN používatelia
Dodávatelia
Tretie strany

Súkromné aj mobilné zariadenia



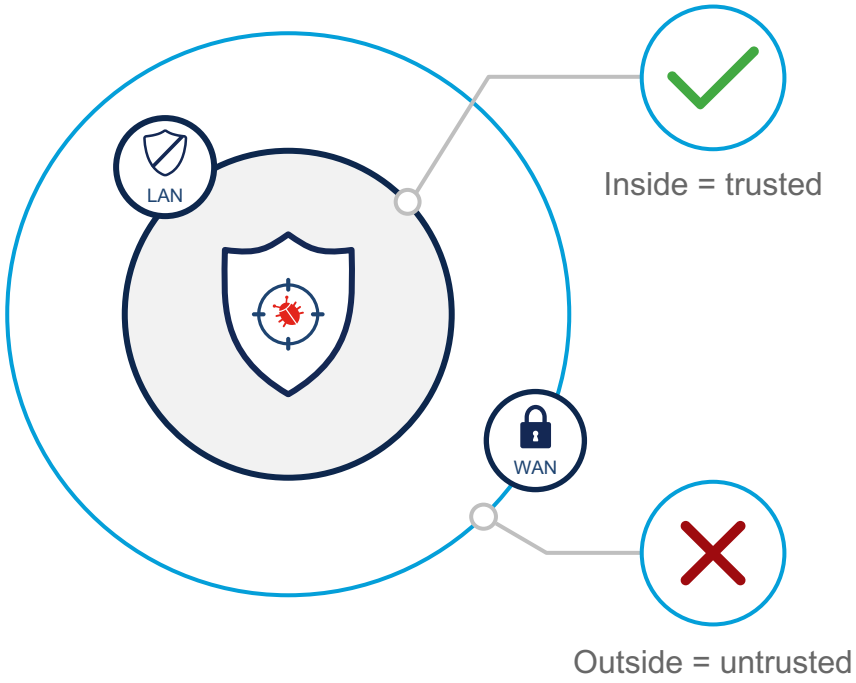
IoT zariadenia

SaaS & Cloud aplikácie

Hybridná Infraštruktúra

Cloud Infraštruktúra

Ako vyzerá bezpečnostný perimeter?



Prístup na princípe ochrany perimetru

Tento prístup k zabezpečeniu podnikových sietí predpokladal, že:

- Overenie iba na vstupe z externého prostredia je postačujúce.
- Každé koncové zariadenie je vlastnené, vydávané a spravované podnikom.
- Všetky zariadenia a aplikácie sú na známych a predvídateľných miestach, najčastejšie za firewallom.
- Zariadenia v sieti si môžu navzájom dôverovať.

Výzvy pre organizácie

Neautorizovaný prístup, identifikácia zraniteľností a medzery vo viditeľnosti

Ako vieme, že používatelia sú tie osoby, za ktoré ich naozaj pokladáme?

Sú ich zariadenia zabezpečené a aktualizované ?

Čo je pripojené do siete? Ako sa to pripojilo?

Priveľa dôvery!

Aké dáta sú v cloud-e? Kto/čo má k dátam prístup?

Ako zabezpečiť a auditovať všetky pripojenia?

Čo existuje v cloude? Ako sa to pripája?

Dnešné hrozby ako výsledok prílišnej dôvery

Potrebujeme iný uhol pohľadu na implementáciu bezpečnosti – “dôveruj, ale preveruj”

Cieľ: Identita

81% úspešných útokov využíva kompromitované účty

Cieľ: Aplikácia

54% zraniteľností web aplikácií má verejne dostupný exploit

Cieľ: Zariadenie

300% nárast rôznych verzií malvéru cieleného na IoT

Päť základných princípov Zero Trust

- Sieť sa považuje vždy za nepriateľskú
- Hrozby existujú v rovnakej miere v internej a aj externej sieti
- O dôvernosti siete sa nemôžeme rozhodovať iba na základe lokality
- Všetky zariadenia, užívatelia a dátové toky musia byť overené a autorizované
- Bezpečnostné politiky musia byť dynamické a vzniknúť z čo najväčšieho počtu zdrojov

https://www.actiac.org/system/files/ACT-IAC%20Zero%20Trust%20Project%20Report%2004182019.pdf

Zero Trust

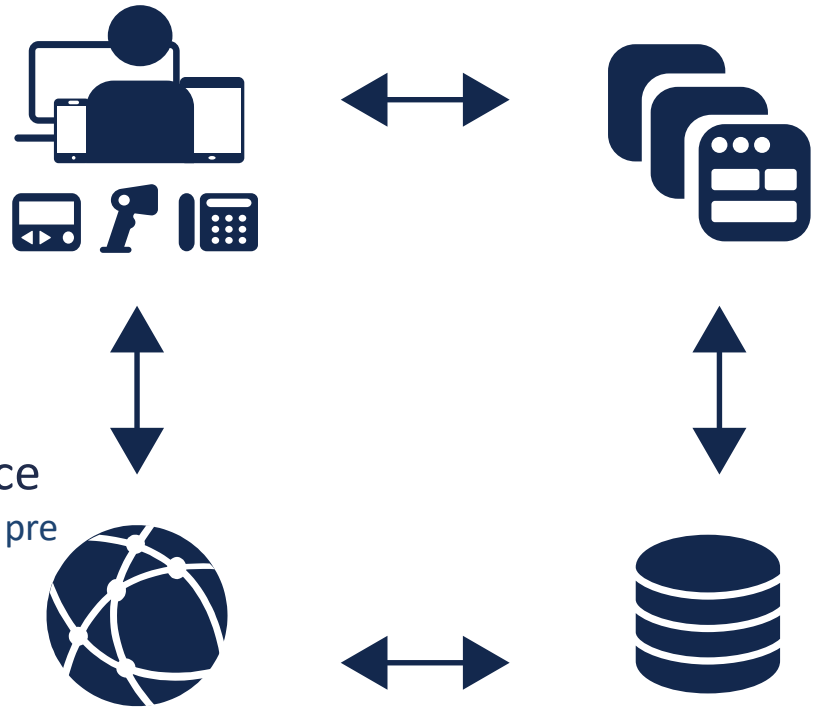
Jeden produkt

Cisco Zero Trust

Dôveryhodný a bezpečný prístup používateľov k aplikáciám a dátam, kedykoľvek a z akéhokoľvek miesta.

Duo pre Workforce

Len dôveryhodné zariadenia a oprávnení používateľia môžu pristúpiť k IT aktívam.



SD-Access pre Workplace

Uplatní “least-privilege” prístup pre všetkých používateľov a všetky pripojené zariadenia.

Tetration pre Workload

V prístupe k aplikáciám zohľadní riziká vs. potreby biznisu, aj v amulti-cloud prostredí.

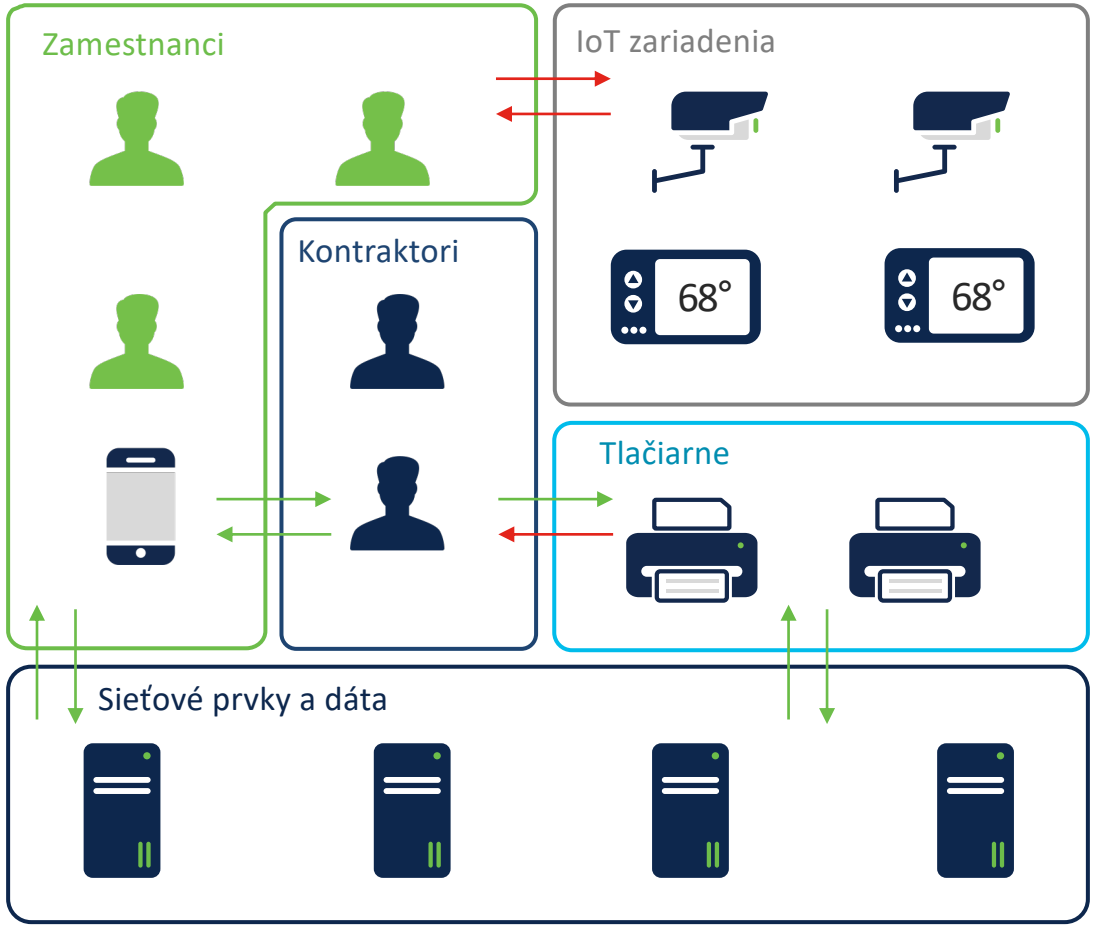
Uplatní pravidlá podľa bezpečnostnej politiky

Ukážka Zero Trust v Cisco

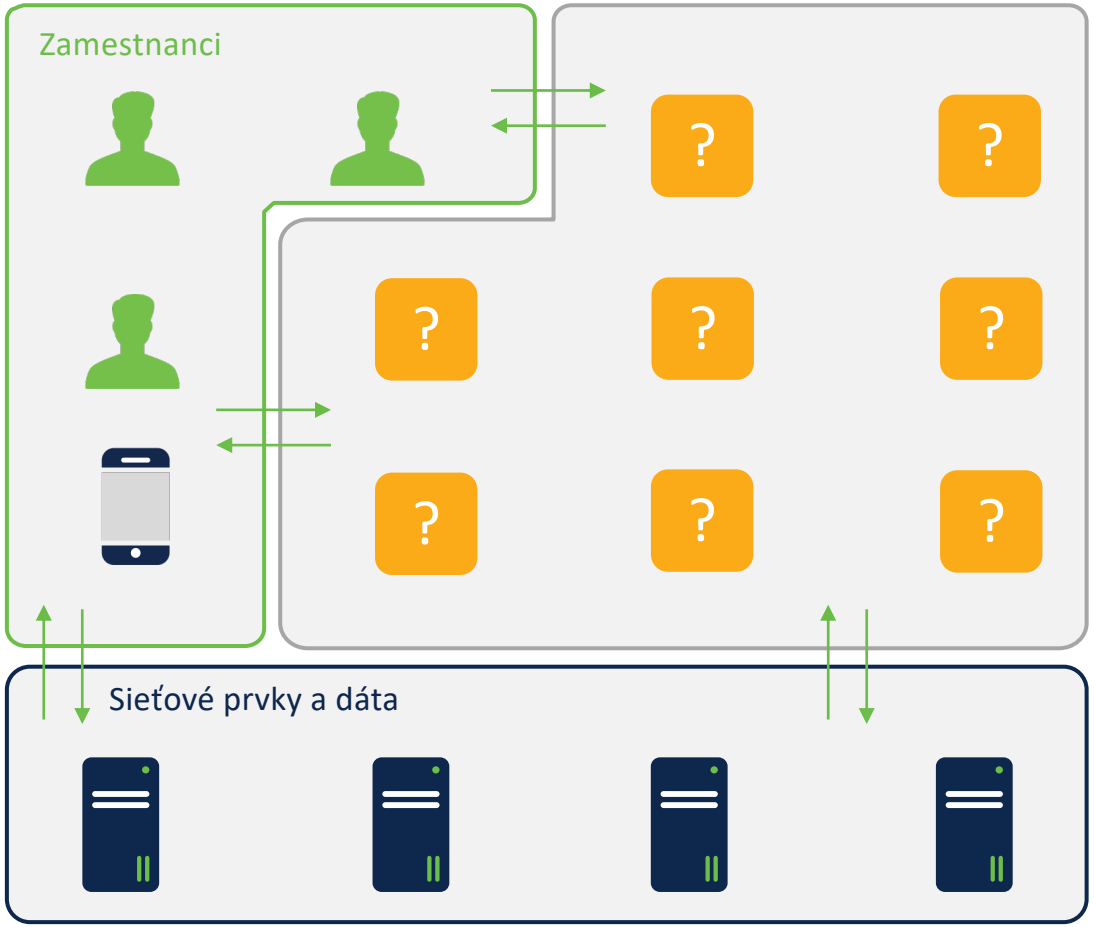
Dôvera sa získava, nie dáva

Least Privilege Access: Očakávanie vs. Realita

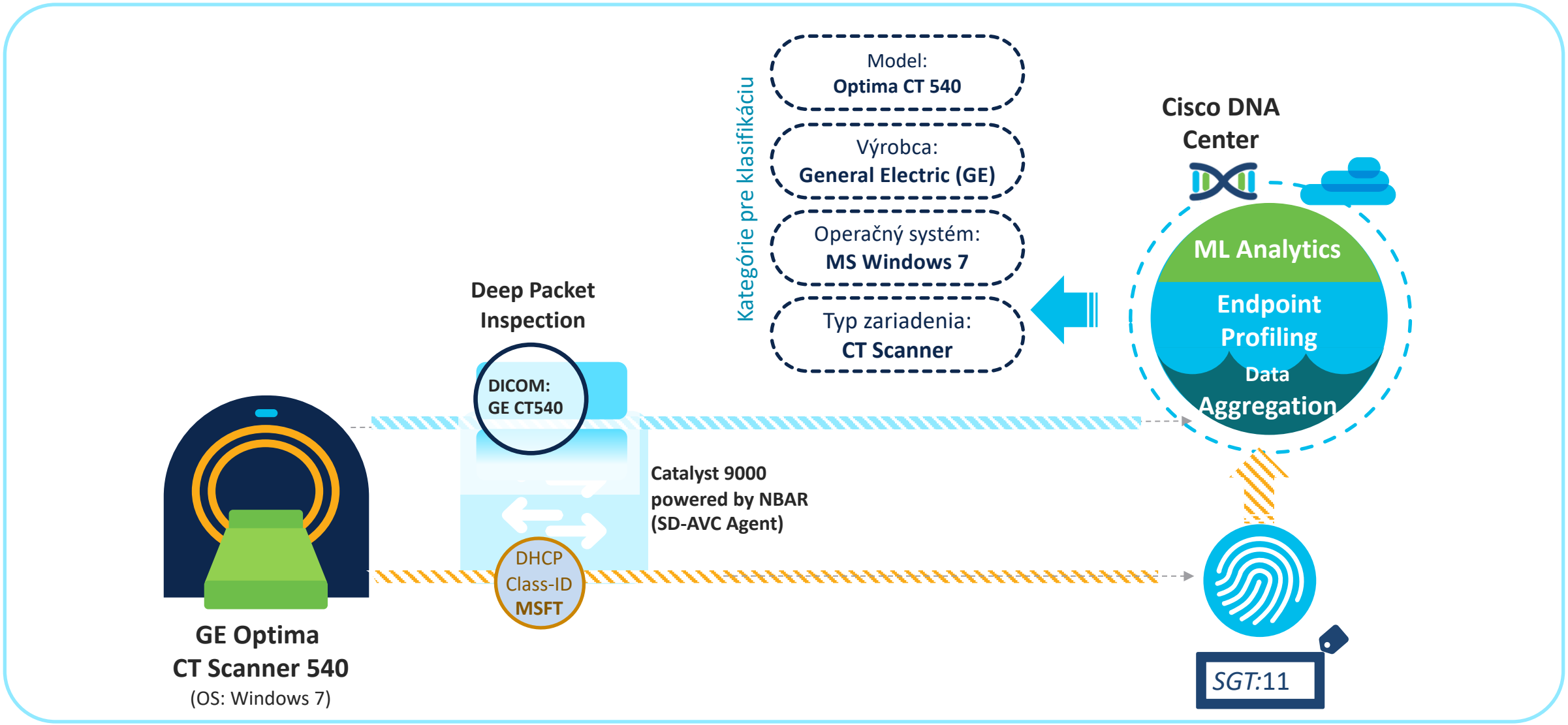
Očakávanie



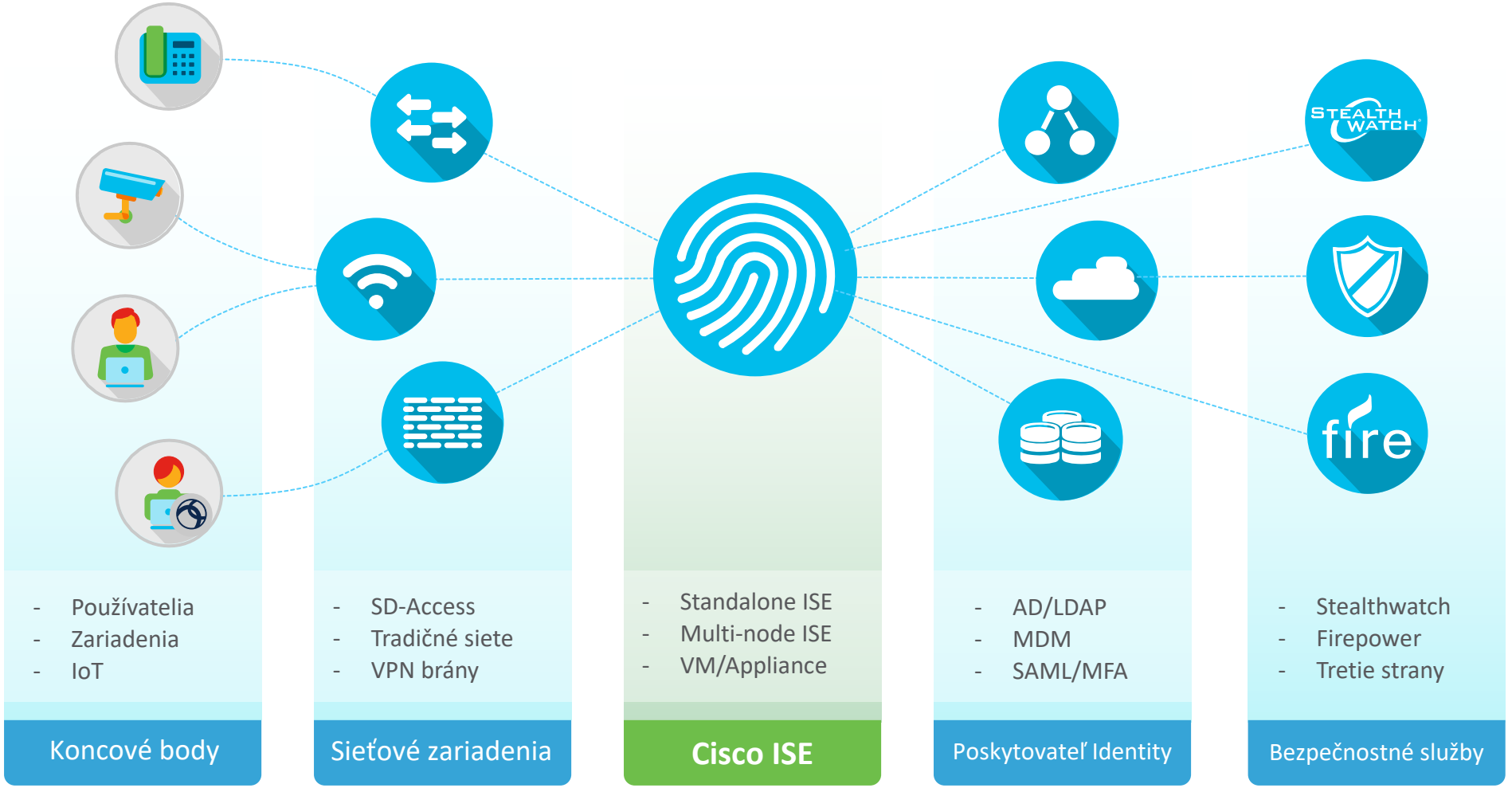
Realita



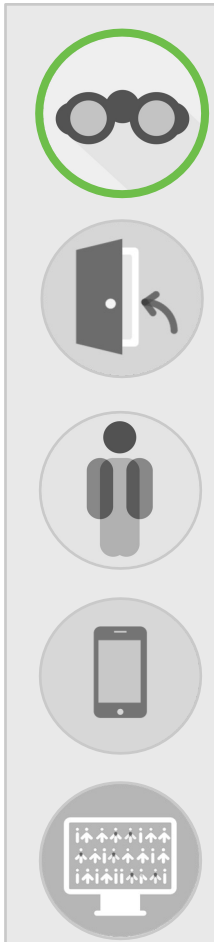
Klasifikácia zariadení prostredníctvom DPI



ISE: Centrálna správa politík na báze identity



Využite viac ako len IP adresu



Pravidlá pomocou IP adries		Pravidlá obohatené o kontext
IP adresa: 192.168.2.101	Kto?	Kristína (zamestnanec)
N/A	Čo?	Lenovo Windows 10
N/A	Kedy?	7:00 CET
N/A	Kde?	Recepcia, Súkromná poliklinika Nitra
N/A	Ako?	Ethernet LAN
N/A	Aplikácie?	Firefox, NIS, AnyConnect
N/A	Atribúty?	✓ Splnená bezp. previerka (NAC)
Takmer neobmedzený prístup 	VÝSLEDOK	**Autorizovaný prístup** 

N/A

Bez ISE

KNOWN

Spolu s ISE

Autorizačné pravidlá uplatňujú bezpečnostnú politiku

Autorizácia len IP adresou vs autorizácia pomocou SGT (Scalable Group Tags)

Pravidlo z firemnej bezpečnostnej politiky:

- Len zamestnanci majú web prístup na Intranet servery

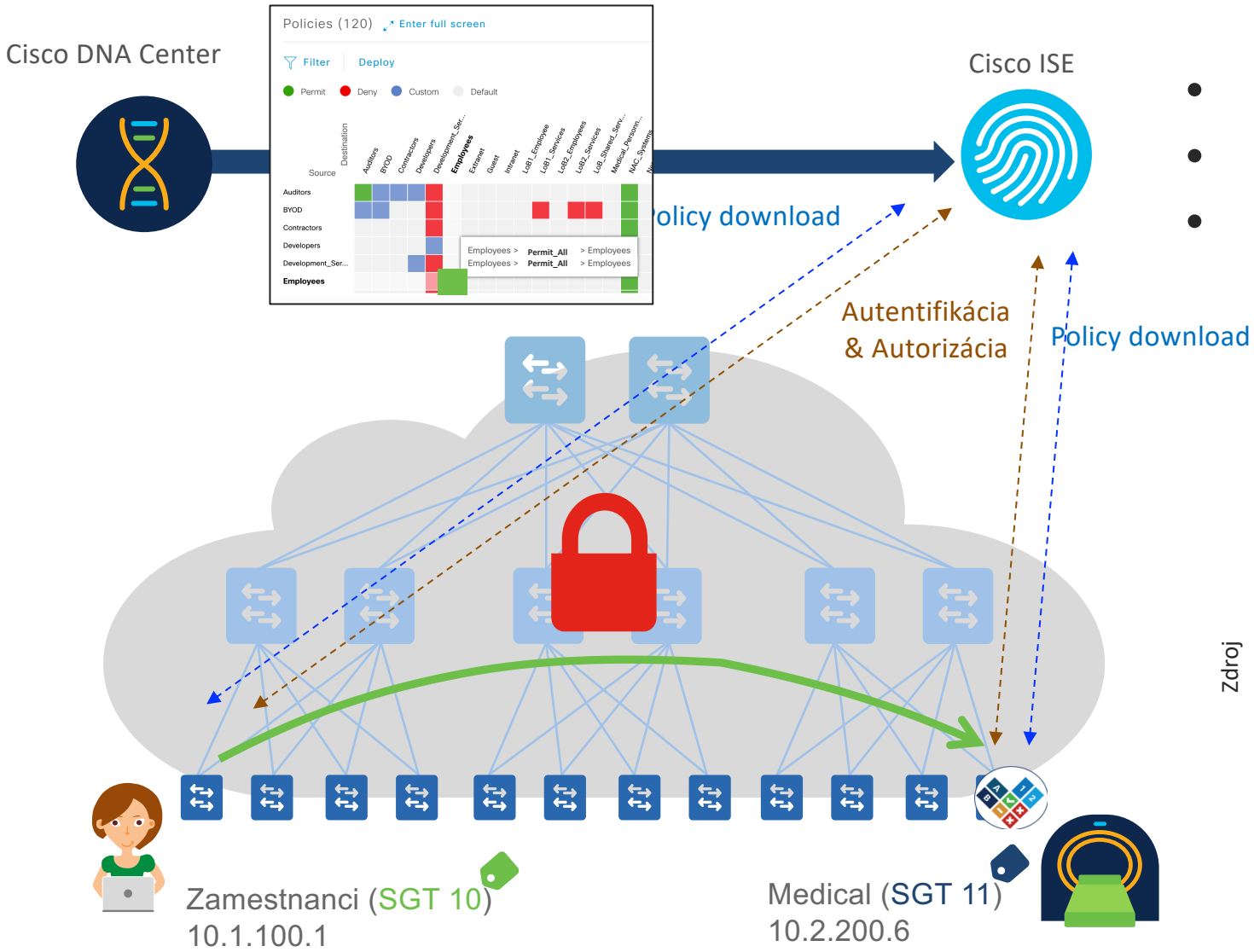
Segmentácia pomocou IP adries

```
Catalyst9000-1#show ip access-list
Extended IP access list CorpPolicy
    10 permit tcp 10.1.100.0 0.0.0.255 172.16.100.0 0.0.0.255 eq 80
    20 permit tcp 10.1.100.0 0.0.0.255 172.16.100.0 0.0.0.255 eq 443
    30 permit tcp 10.2.101.0 0.0.0.255 172.16.100.0 0.0.0.255 eq 80
```

Segmentácia pomocou SGT

```
Catalyst9000-1#show cts role-based permissions
IPv4 Role-based permissions from 10:Zamestnanci to 100:Intranet: Len_Web-10
```

Ako to spolu všetko funguje?

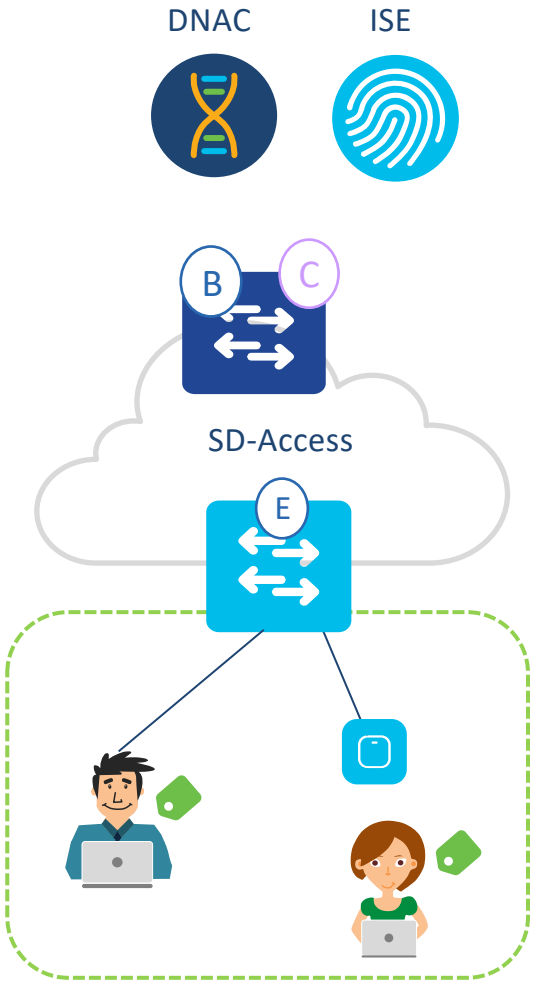


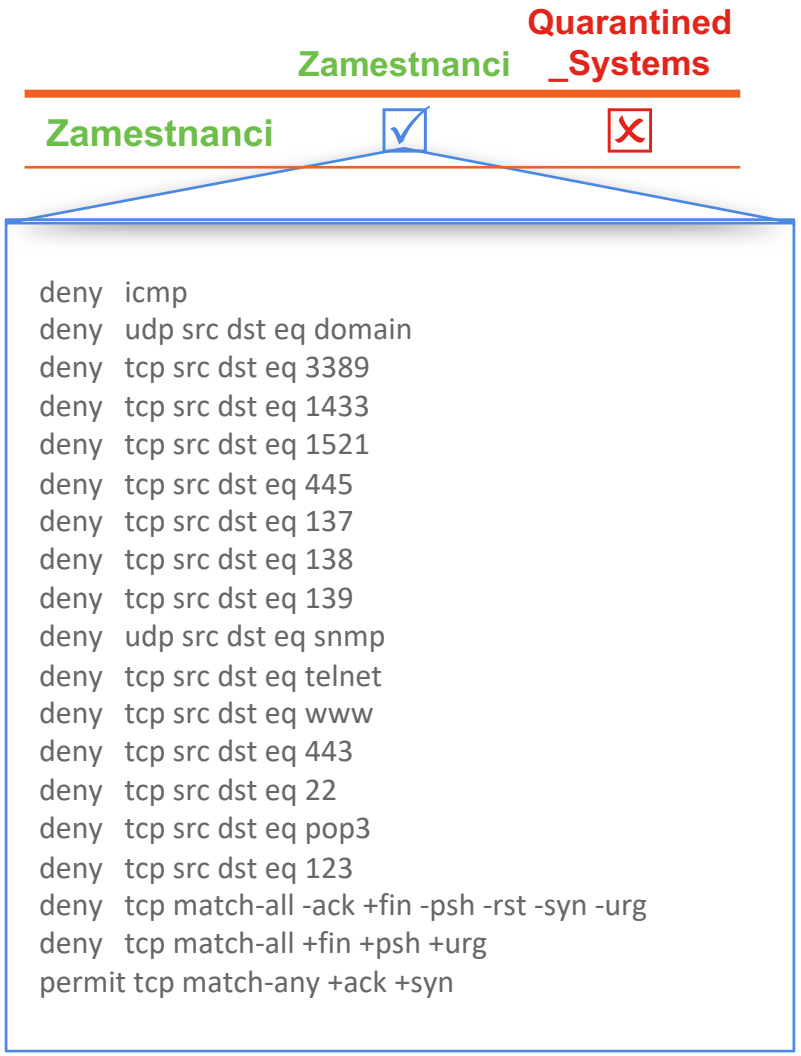
- Autentifikácia & Autorizácia: ISE
- Propagácia: SGT vo VXLAN
- Vynútenie: Egress Fabric Edge

Pravidlá bezpečnostnej politiky	Cieľ: Zamestnanci	Cieľ: Medical
Zdroj: Zamestnanci	Permit All	Deny All
Zdroj: BYOD	Permit All	Deny All
Zdroj: Medical	Deny All	Permit All
Zdroj: Doktori	Deny All	Permit All

Príklad použitia: Mikrosegmentácia

Ochrana proti “lateral movement” a “privilege escalation”

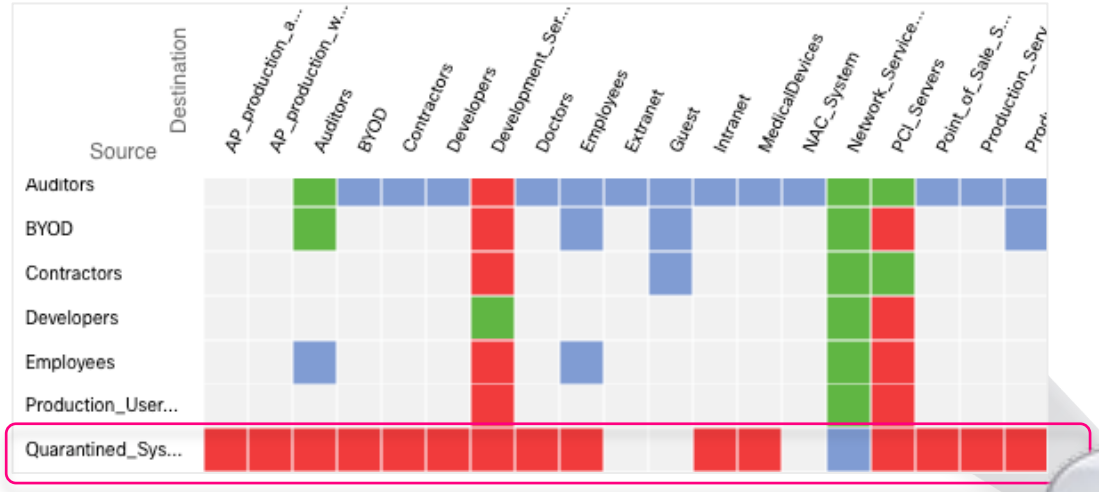




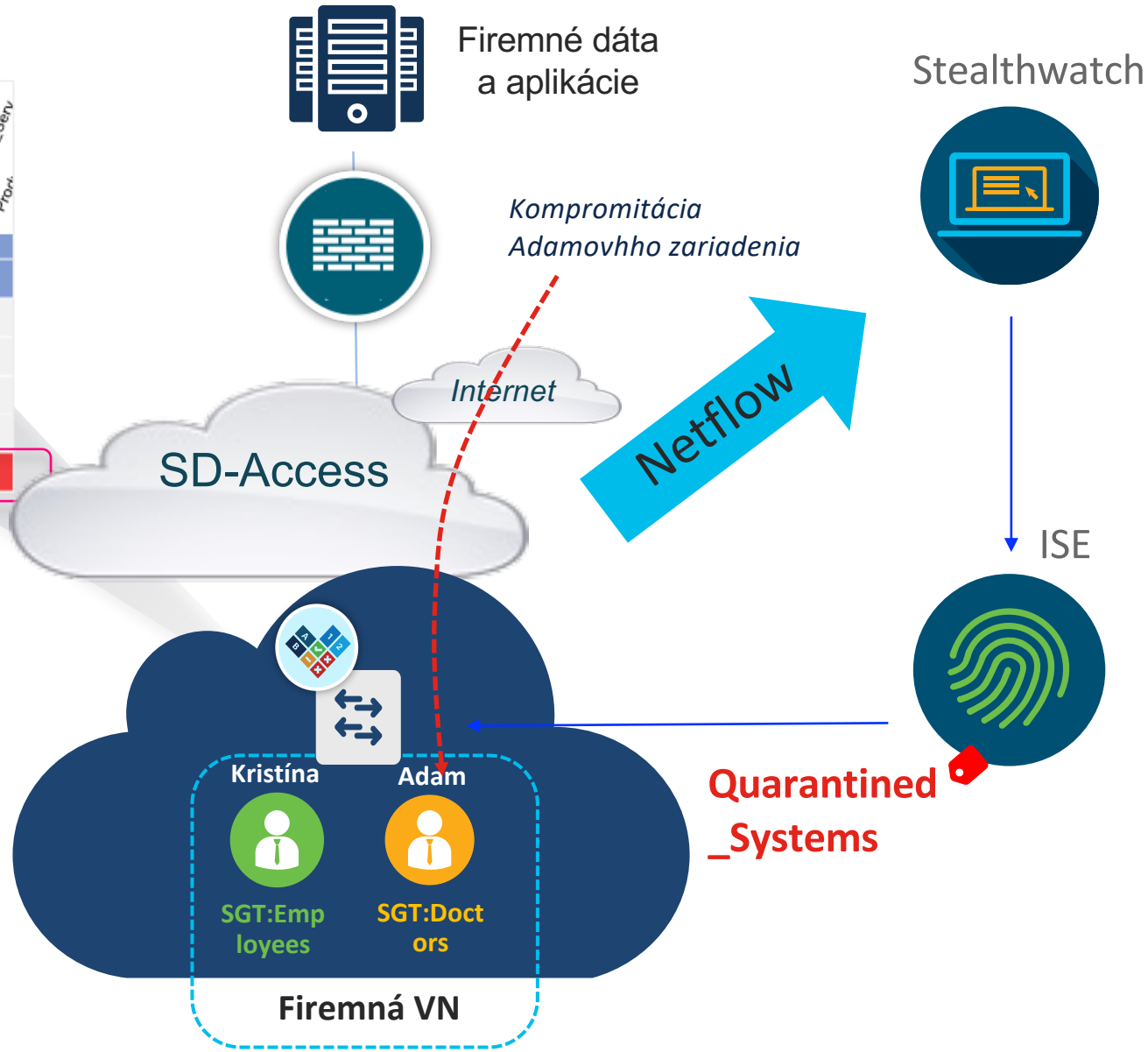
- Dynamické pridelenie úrovne dôvery používateľom a zariadeniam
- Dynamické vynútenie autorizačných pravidiel podľa úrovne dôvery
- Blokovanie plošného šírenia malvéru a zamedzenie eskalácie privilégií

Neustála verifikácia úrovne dôvery

Rapid Threat Containment

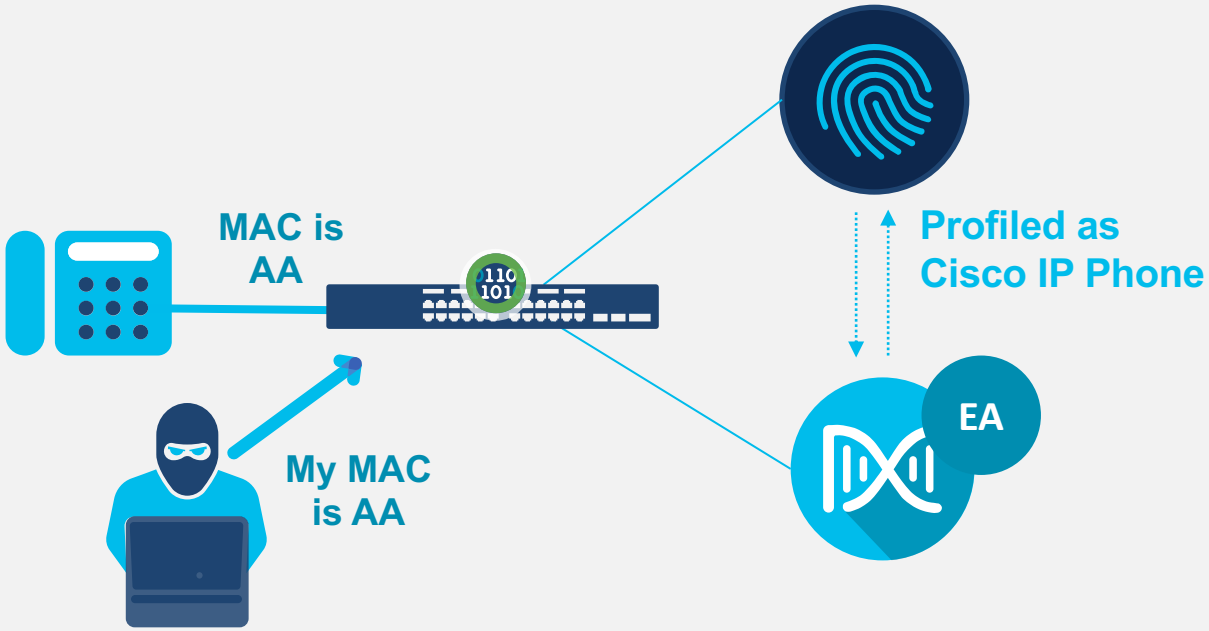


- Kompromitovaným zariadeniam automaticky nedôverujem, čo sa premietne do zmeny SGT.
- Na základe zmeneného SGT sa automaticky aplikujú autorizačné pravidlá, ktorými blokujem prístup k firemným dátam a aplikáciám.



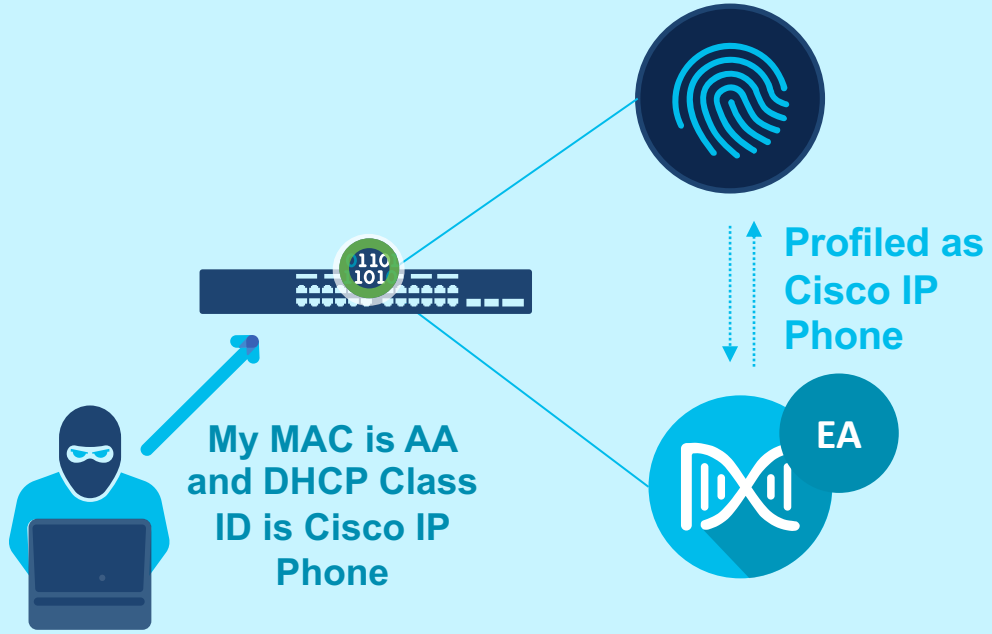
Problém: Odcudzenie identity falšovaním MAC/atribútov

MAC Spoofing



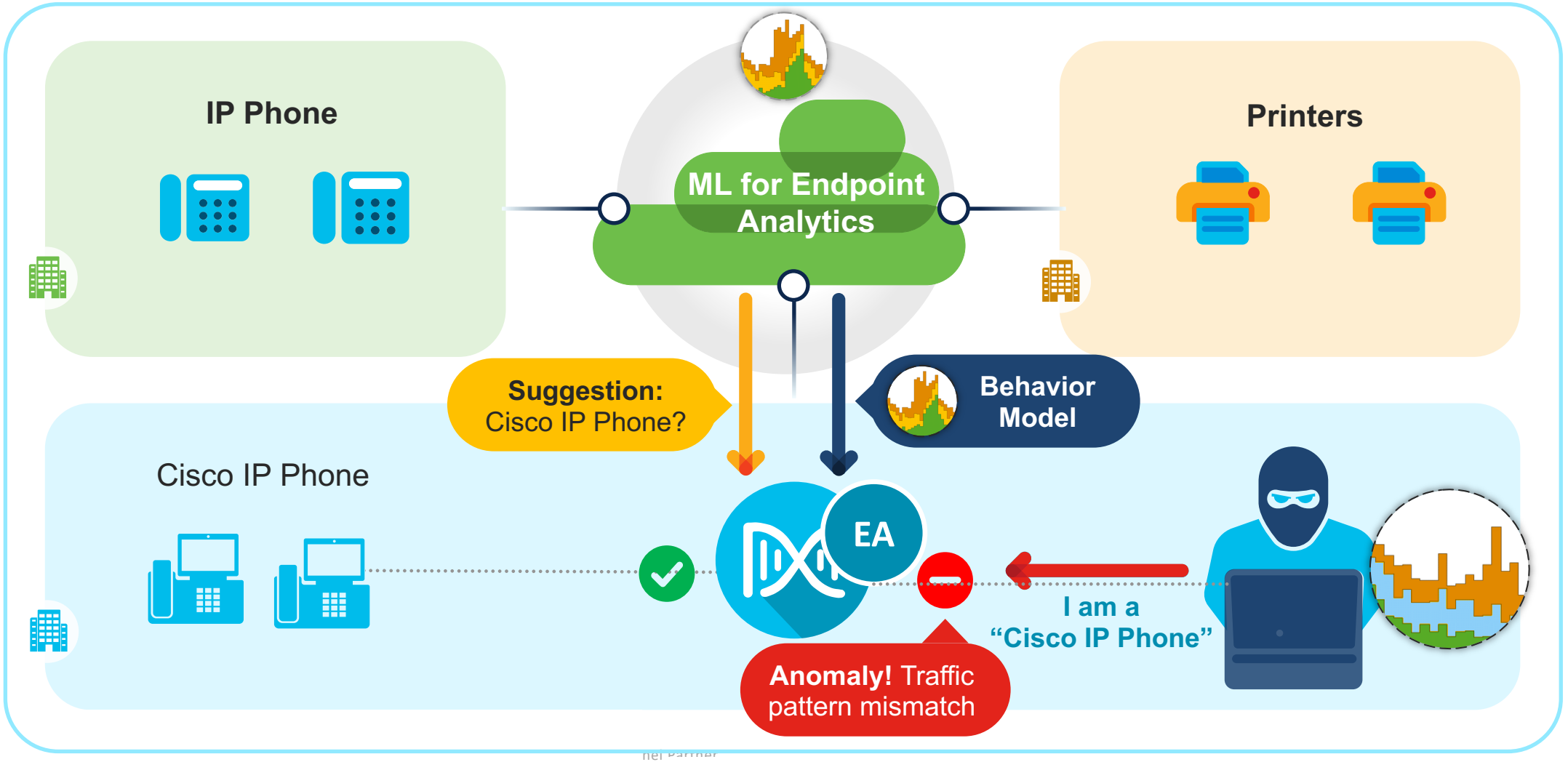
Ukradnutie MAC adresy iného, už autorizovaného zariadenia za účelom získania rovnakých privilégií

Attribute Spoofing



Ukradnutie kompletnej identity MAC/typ zariadenia na získanie privilegovaného prístupu do siete

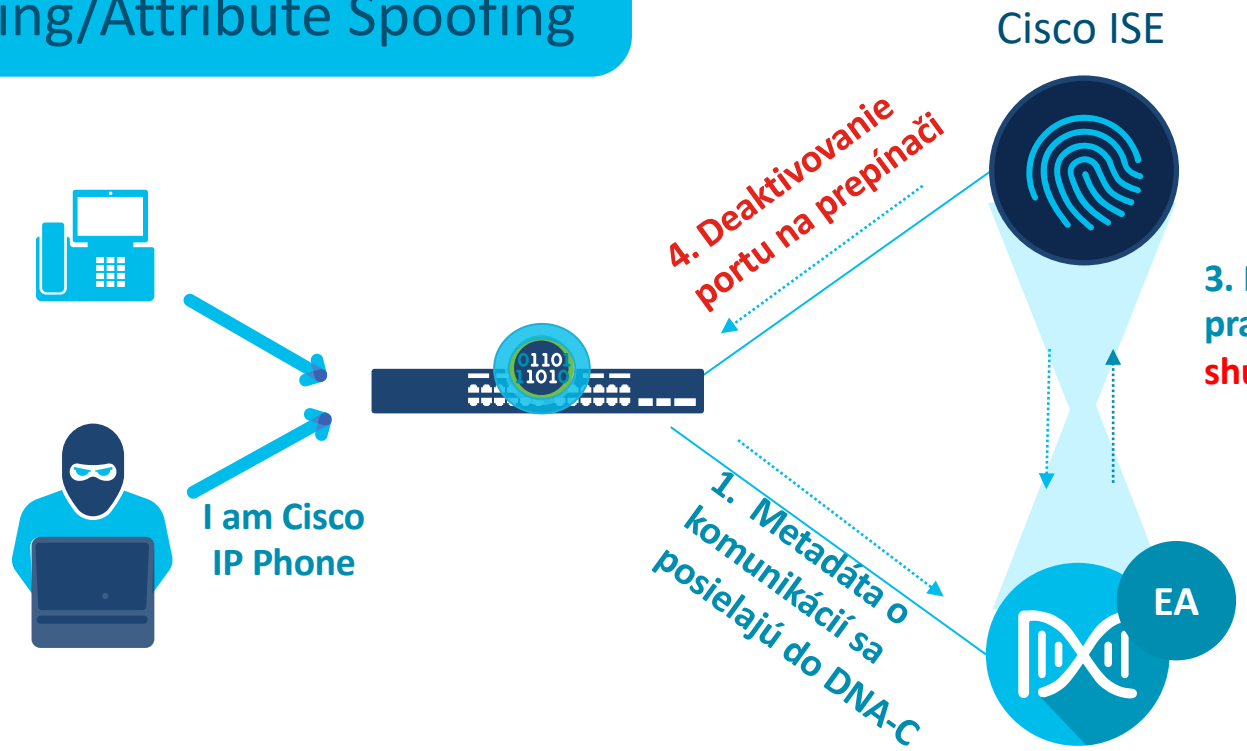
Detekcia falšovania pomocou AI Spoofing Detection

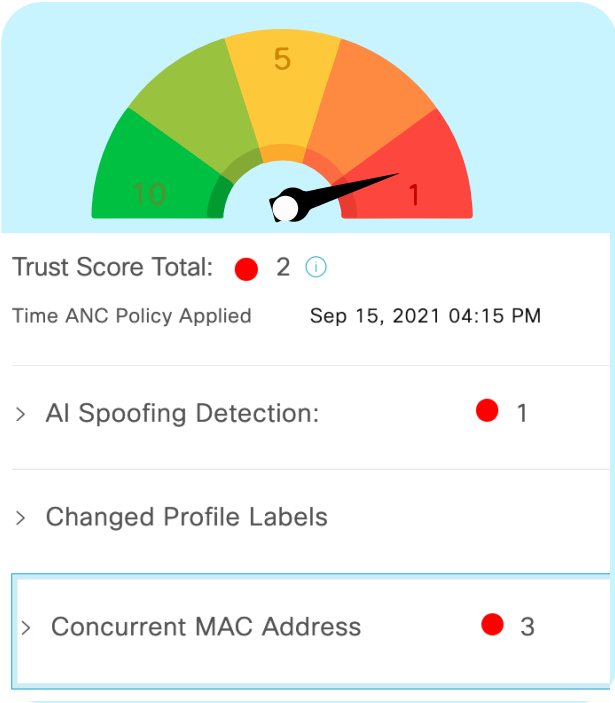


EA: Endpoint Analytics

Detekcia podvrhnutia identity zariadenia

MAC Spoofing/Attribute Spoofing





Concurrent MAC Detection + Identify Profile Label Change (DNAC 2.2.3)

AI Spoof Detection (supported in DNAC 2.2.2)

SGT komunikuje úroveň dôvery naprieč celou IT infraštruktúrou

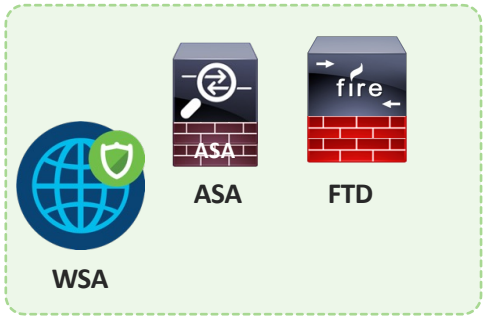
Security

Identity Services Engine / Cisco DNA Center

APIC-DC (ACI Controller)

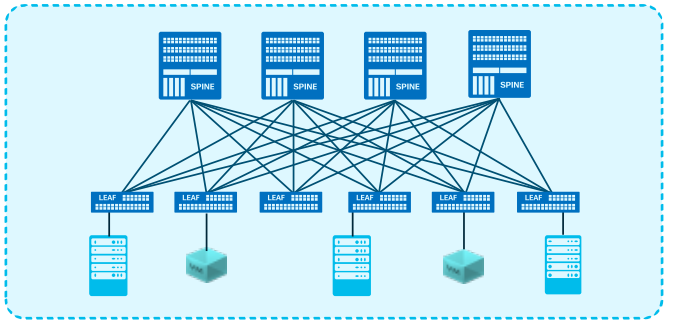
Spoločné bezpečnostné skupiny

Bezpečnostné prvky



IT infraštruktúra, SD-Access, SD-WAN

Dátové centrum, Cloud

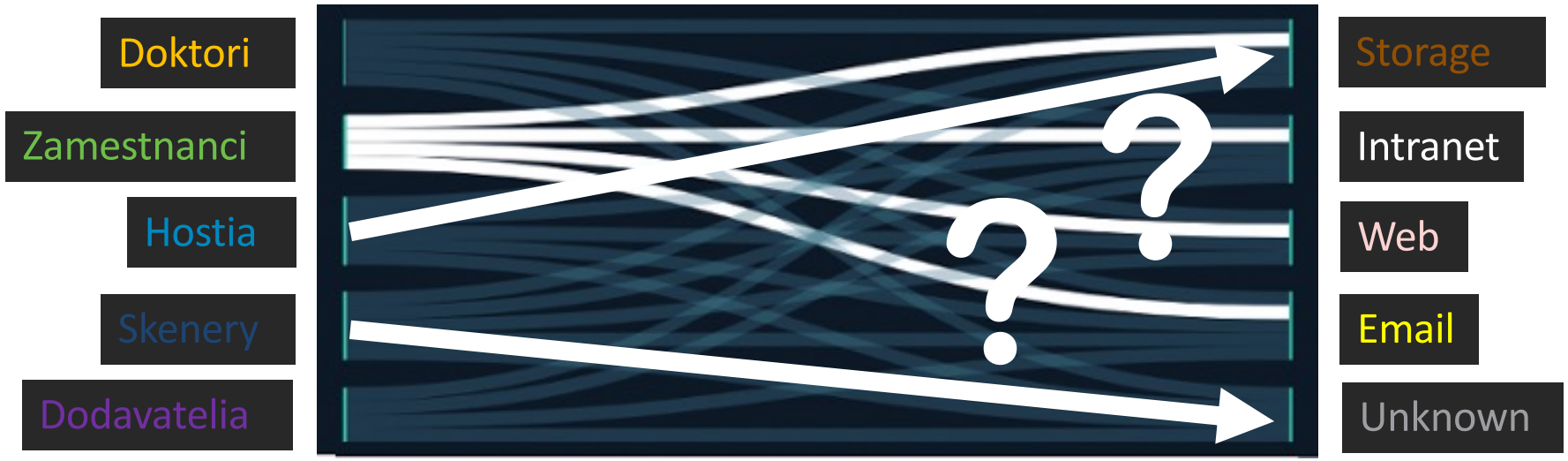


Softvérovo Definovaná Segmentácia

Audit komunikácie medzi SGT skupinami

ZDROJOVÉ
SGT Skupiny

CIEĽOVÉ
SGT Skupiny



Cisco DNA Center **Group Based Policy Analytics**:

- Zobrazí komunikačné toky medzi jednotlivými skupinami

cisco SECURE

Ďakujem za pozornosť