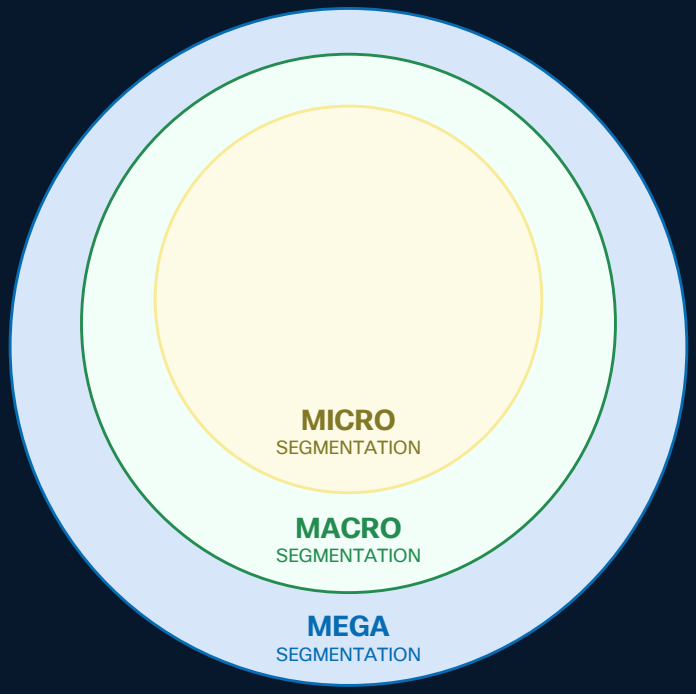
OD MAKRA K MIKRO, OD IP K IDENTITÁM: EVOLÚCIA SEGMENTÁCIE V CAMPUSOCH A DÁTOVÝCH CENTRÁCH V ÉRE ZERO TRUST

Tomáš Ondovčík

Network Segmentation Use cases



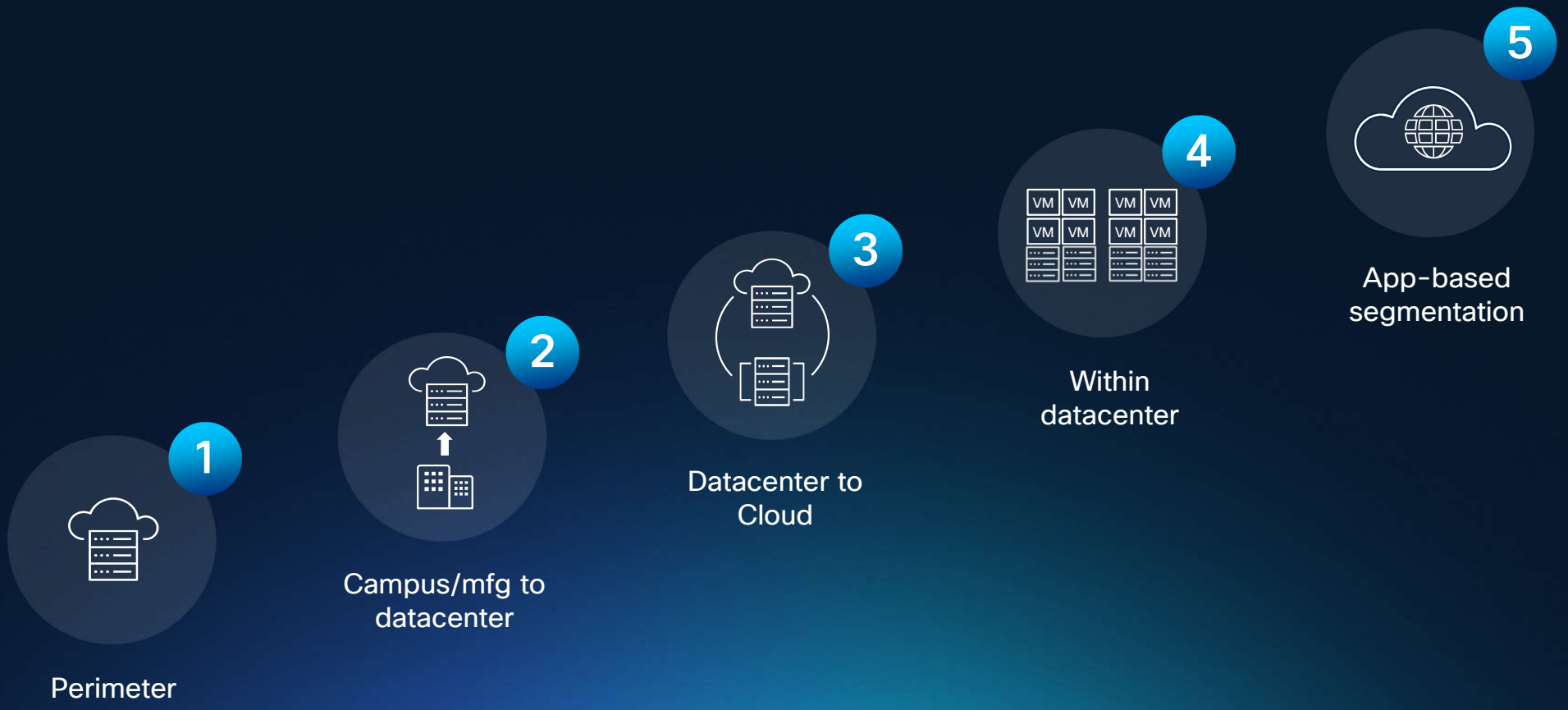
Network Segmentation Spectrum

Mega Segmentation (The Perimeter)
- Broadest level of isolation (inside / outside boundary).
- Focuses on North-South traffic (Internet vs. Enterprise) and major domain separation (e.g., Data Center vs. Campus).

Macro Segmentation (The Zones)
- Logical grouping of assets (using VRFs, VLANs).
- Examples: Dev/Test/Prod, HR/Finance, EMEA/APAC).

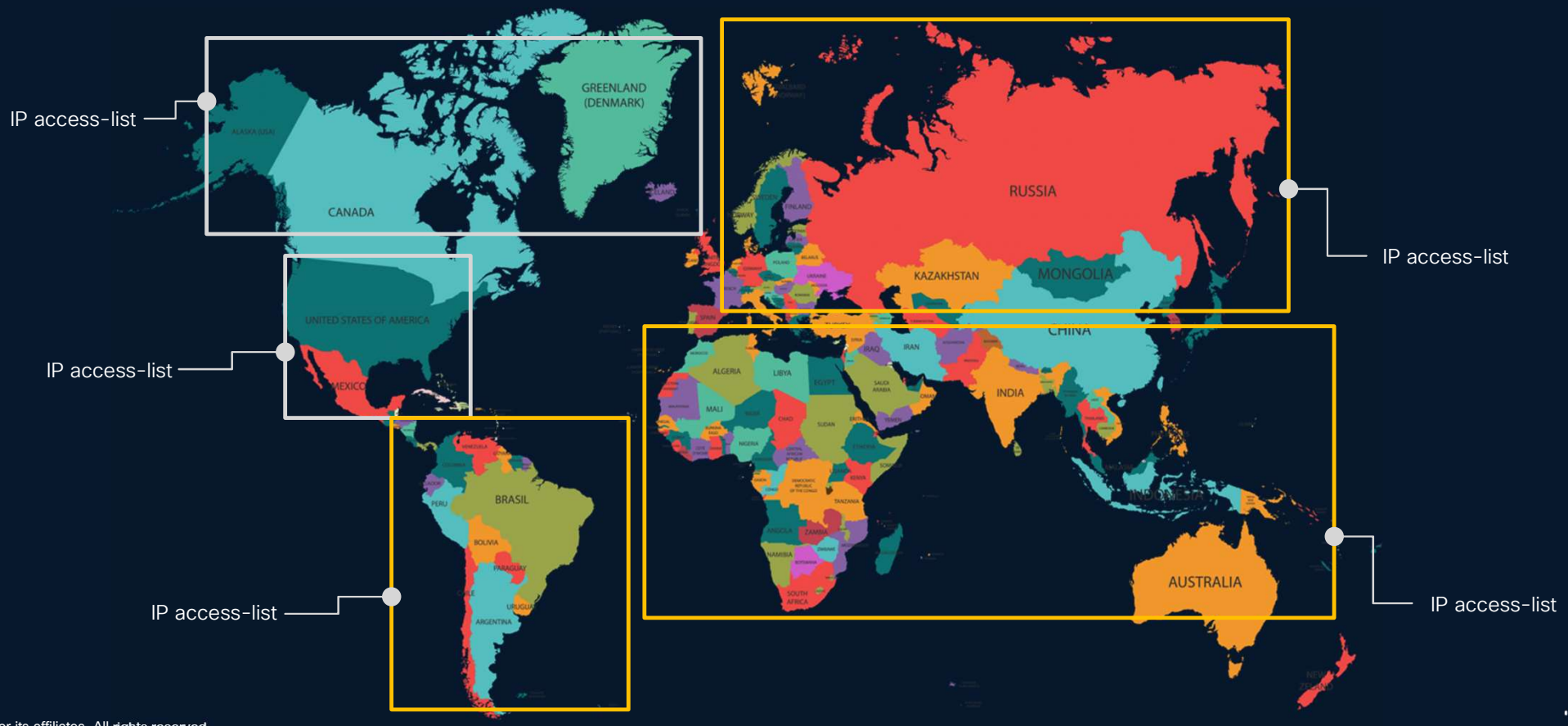
Micro Segmentation (The Identity & Role)
- Granular isolation within a specific macro segment based on identity and function rather than IP addresses.
- Campus: Isolate users, devices, and IoT endpoints within the same VLAN (using Cisco TrustSec SGTs, VXLAN GPO)
- Data Center: Restricts East-West traffic between individual workloads or application tiers to prevent lateral movement (using Cisco ACI ESG/EPG, VLAN GPO)

Segmentation that meets you where you are



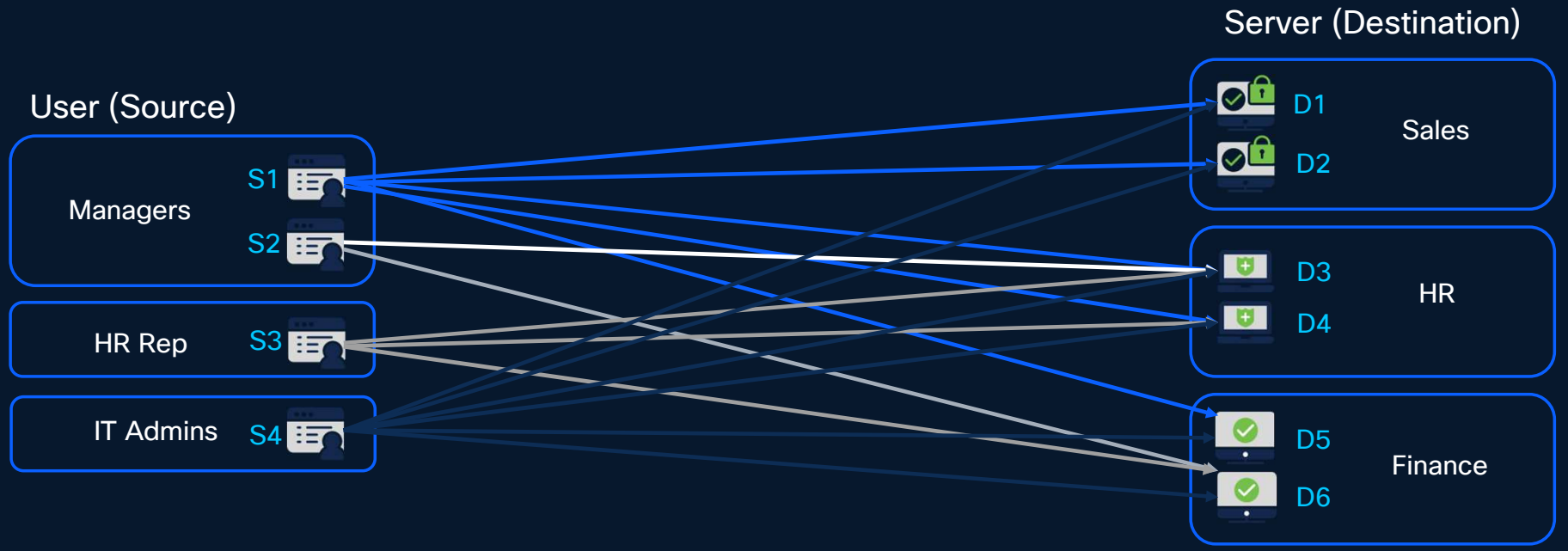
Campus

Traditional Segmentation



What is the issue?

Traditional Segmentation



Number of ACL's:

(# of Sources) * (# of Destinations) * Permissions = # of ACEs

Src (S1) * Dst (D1~D6) * Permission (4) = 24 ACEs for S1

Src (S1~S4) * Dst (D1~D6) * Permission (4) = 96 ACEs for S1~S4

What is the issue?

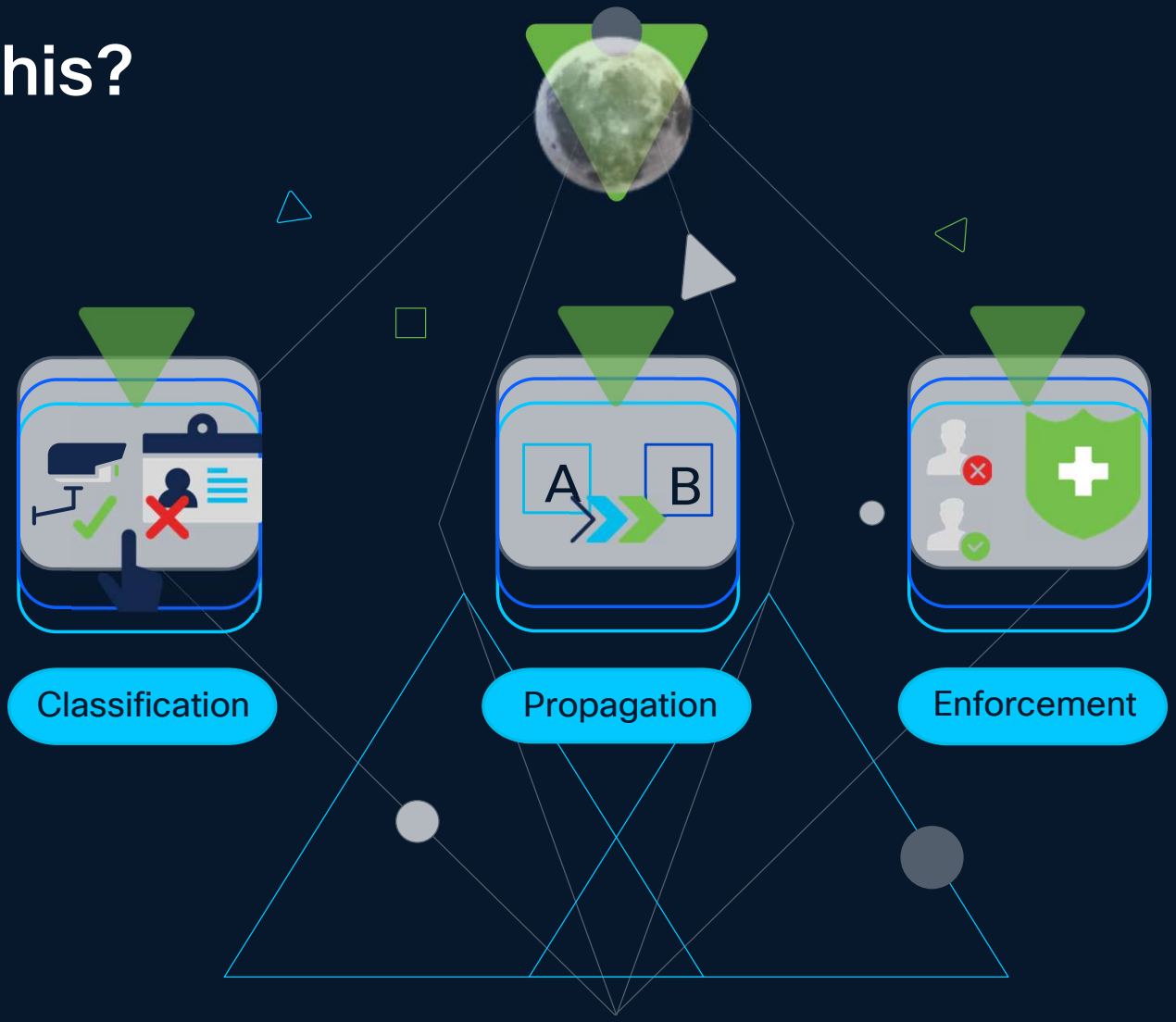
Traditional Segmentation – We lack the business intent

```
access-list 102 permit tcp 100.126.4.49 0.255.255.255 lt 1449 28.237.88.171 0.0.0.127 lt 3679
access-list 102 deny icmp 157.219.157.249 255.255.255.255 gt 1354 60.126.167.112 0.0.31.255 gt 1025
access-list 102 deny icmp 76.176.66.41 0.255.255.255 lt 278 169.48.105.37 0.0.1.255 gt 968
access-list 102 permit ip 8.88.141.113 0.0.0.127 lt 2437 105.145.196.67 0.0.1.255 lt 4167
access-list 102 permit udp 60.242.95.62 0.0.31.255 eq 3181 33.191.71.166 255.255.255.255 lt 2422
access-list 102 permit icmp 186.246.40.245 0.255.255.255 eq 3508 191.139.67.54 0.0.1.255 eq 1479
access-list 102 permit ip 209.111.254.187 0.0.1.255 gt 4640 93.99.173.34 255.255.255.255 gt 28
access-list 102 permit ip 184.232.88.41 0.0.31.255 lt 2247 186.33.104.31 255.255.255.255 lt 4481
access-list 102 deny ip 106.79.247.50 0.0.31.255 gt 1441 96.62.207.209 0.0.0.255 gt 631
access-list 102 permit ip 39.136.60.170 0.0.1.255 eq 4647 96.129.185.116 255.255.255.255 lt 3663
access-list 102 permit tcp 30.175.189.93 0.0.31.255 gt 228 48.33.30.91 0.0.0.255 gt 1388
access-list 102 permit ip 167.100.52.185 0.0.1.255 lt 4379 254.202.200.26 255.255.255.255 gt 4652
access-list 102 permit udp 172.16.184.148 0.255.255.255 gt 4163 124.38.159.247 0.0.0.127 lt 3851
access-list 102 deny icmp 206.107.73.252 0.255.255.255 lt 2465 171.213.183.230 0.0.31.255 gt 1392
access-list 102 permit ip 96.174.38.79 0.255.255.255 eq 1917 1.156.181.180 0.0.31.255 eq 1861
access-list 102 deny icmp 236.123.67.53 0.0.31.255 gt 1181 31.115.75.19 0.0.1.255 gt 2794
access-list 102 deny udp 14.45.208.20 0.0.0.255 lt 419 161.24.159.166 0.0.0.255 lt 2748
access-list 102 permit udp 252.40.175.155 0.0.31.255 lt 4548 87.112.10.20 0.0.1.255 gt 356
access-list 102 deny tcp 124.102.192.59 0.0.0.255 eq 2169 153.233.253.100 0.255.255.255 gt 327
access-list 102 permit icmp 68.14.62.179 255.255.255.255 lt 2985 235.228.242.243 255.255.255.255 lt 2286
access-list 102 deny tcp 91.198.213.34 0.0.0.255 eq 1274 206.136.32.135 0.255.255.255 eq 4191
access-list 102 deny udp 76.150.135.234 255.255.255.255 lt 3573 15.233.106.211 255.255.255.255 eq 3721
access-list 102 permit tcp 126.97.113.32 0.0.1.255 eq 4644 2.216.105.40 0.0.31.255 eq 3716
access-list 102 permit icmp 147.31.93.130 0.0.0.255 gt 968 154.44.194.206 255.255.255.255 eq 4533
access-list 102 deny tcp 154.57.128.91 0.0.0.255 lt 1290 106.233.205.111 0.0.31.255 gt 539
access-list 102 deny ip 9.148.176.48 0.0.1.255 eq 1310 64.61.88.73 0.0.1.255 lt 4570
access-list 102 deny ip 124.236.172.134 255.255.255.255 gt 859 56.81.14.184 255.55.255.255 gt 2754
access-list 102 deny icmp 227.161.68.159 0.0.31.255 lt 3228 78.113.205.236 255.55.255.255 lt 486
access-list 102 deny udp 167.160.188.162 0.0.0.255 gt 4230 248.11.187.246 0.255.255.255 eq 2165
```

Security Groups

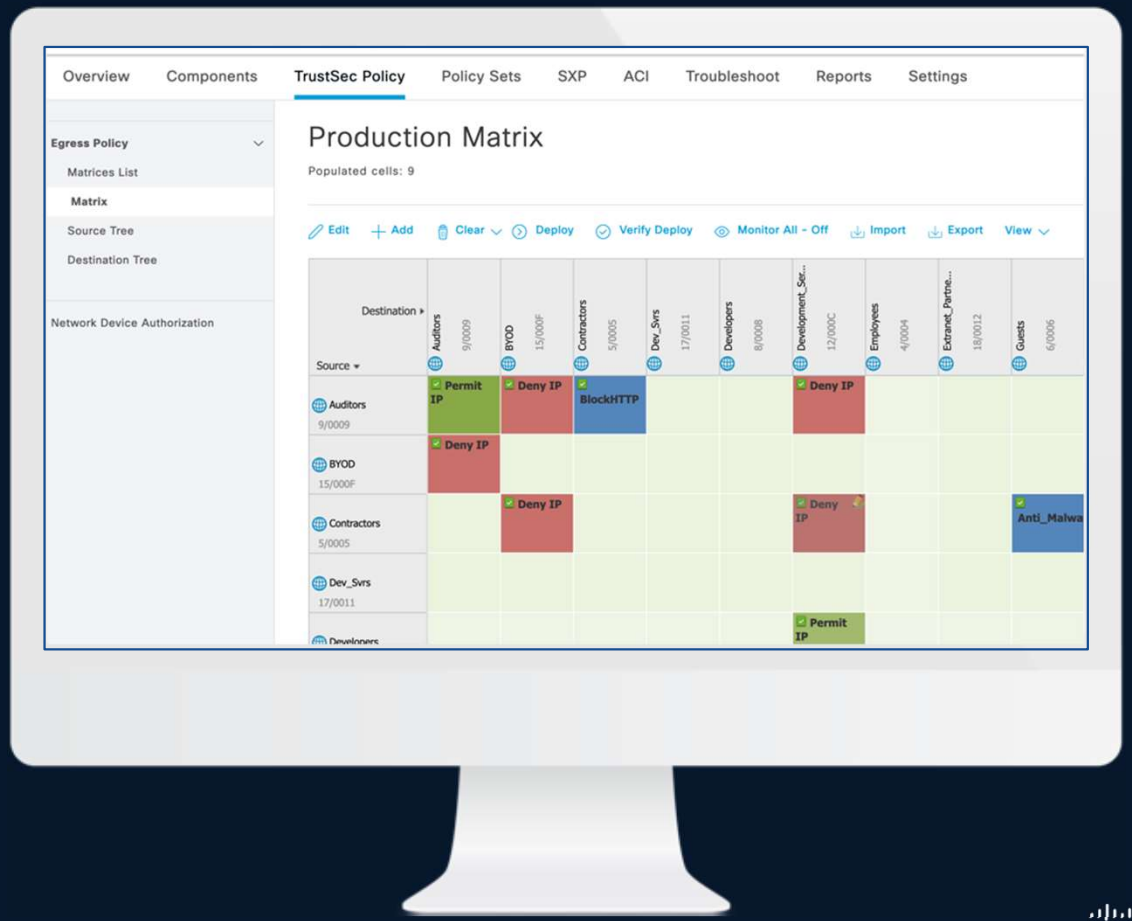
How can we solve this?

TrustSec is a next-generation access control method that can greatly enhance the performance, scalability, and manageability of your network.



TrustSec Matrix

- The TrustSec Matrix is where you define which SGACL is applied per SGT
- The matrix displays source SGTs on the left and destination SGTs on the top
- The intersection of the rows and columns are the actual enforcement instructions based on the SGACL



DC

Segmentation and Policy Control Challenges

Current: Siloed Tools & Policies

Challenges

- Siloed Teams & Tools
- Inconsistent Policies
- Lack of Visibility & Control

Protecting workloads at network AND process level

Network level segmentation | Process level segmentation

Data Center Edge (Perimeter) Firewall

A DC perimeter firewall primarily

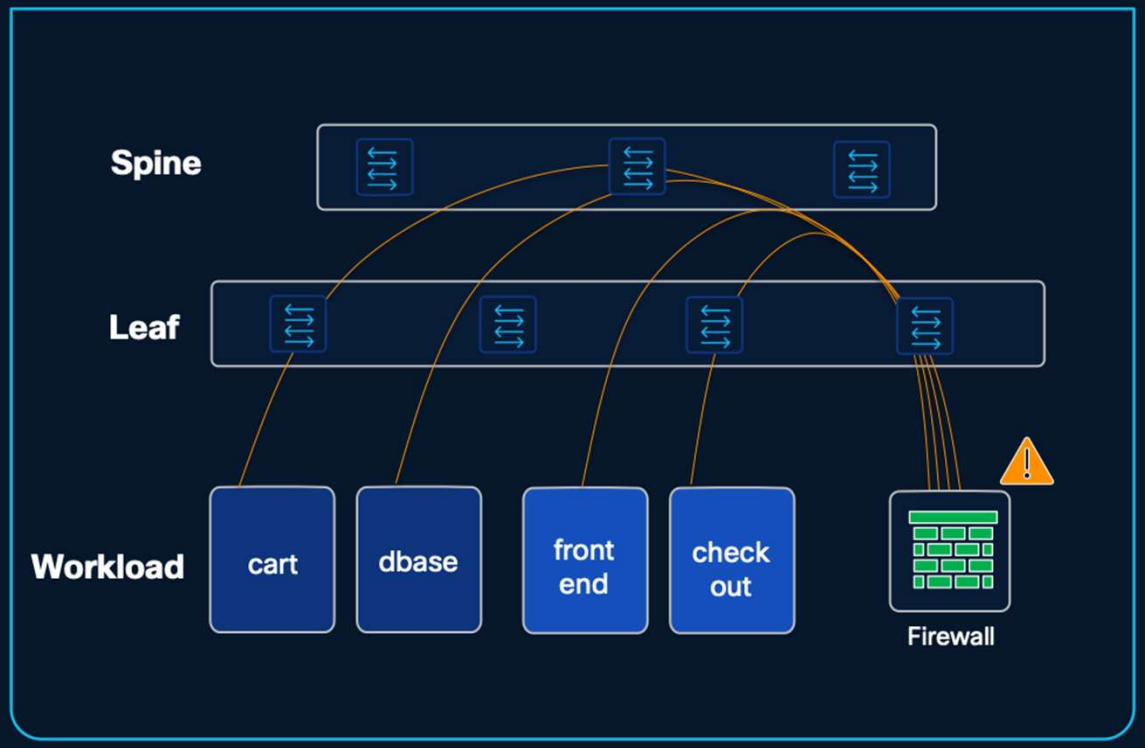
protects *north-south* traffic by blocking external threats, scale + efficacy

securing critical workloads, enforcing least-privilege access, supporting *compliance, and ensuring business continuity.*

supports *advanced application-aware security, encrypted traffic inspection*,

Traffic management complexity moving traffic to and from firewall clusters

Traditional architecture creates east-west bottlenecks



Firewalls excel at perimeter defense and compliance

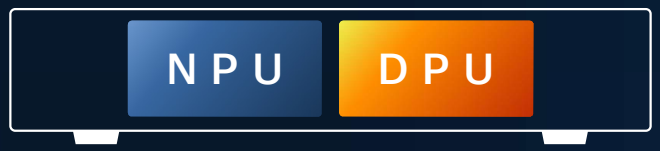
- IPS/IDS
- URL Filtering
- NAT, Identity, others.

But lateral traffic defense needs a different approach

- Hair pinning adds latency
- Architectural limits create visibility gaps
- Scaling east-west security is costly

cisco

SMART SWITCH

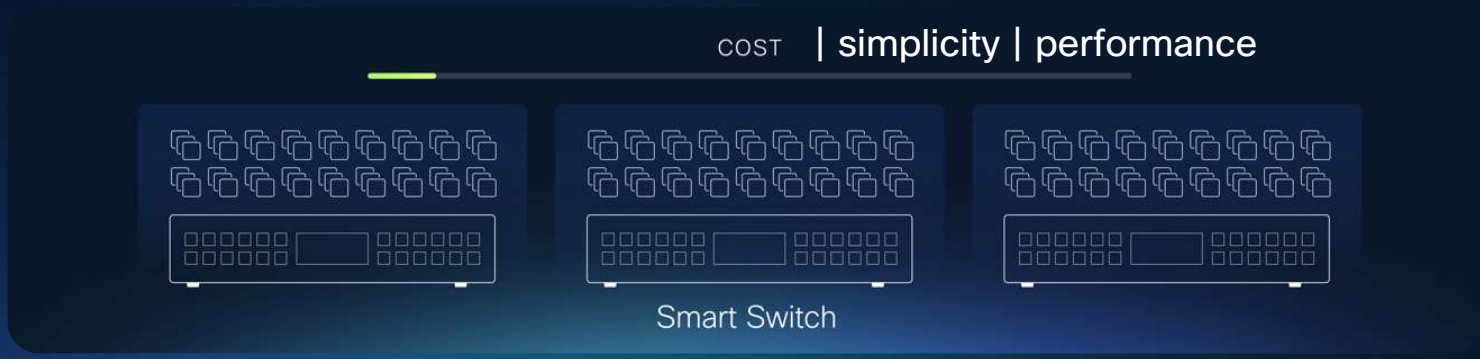


Inspecting packets

Moving packets from A to B

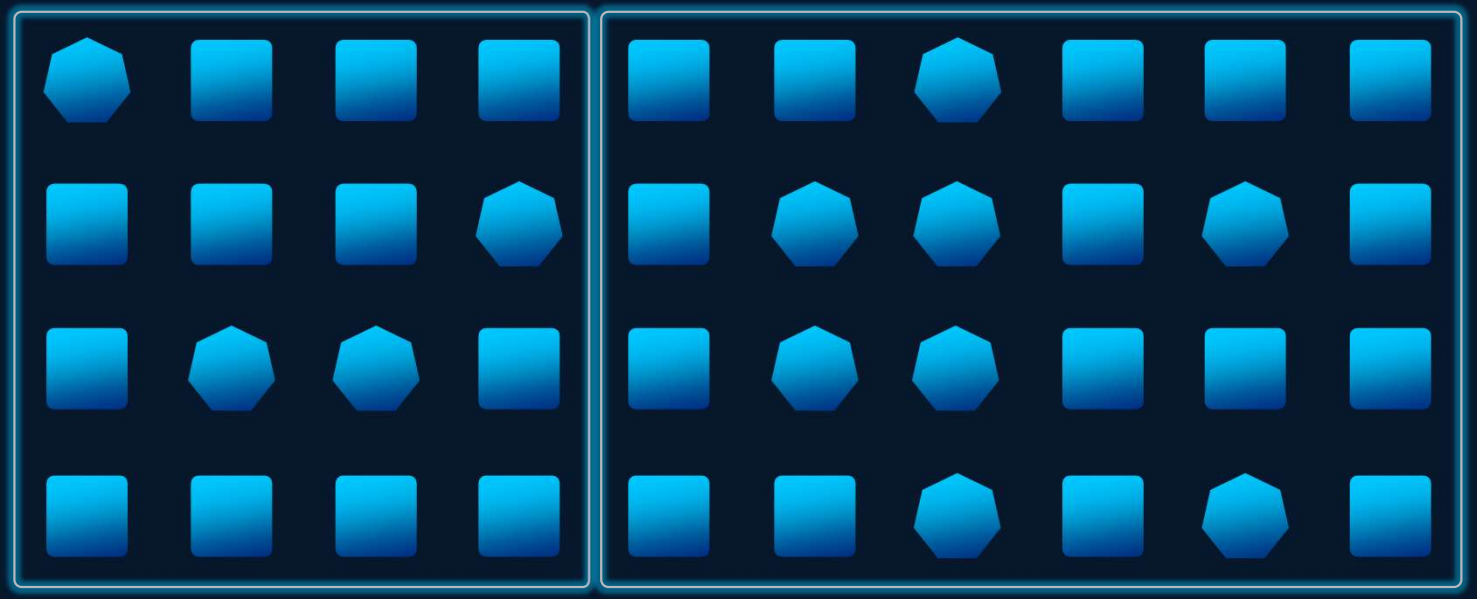
Firewall
on every server port

Top of Rack Smart Switch
on every server port



MACROSEGMENTATION

MICROSEGMENTATION



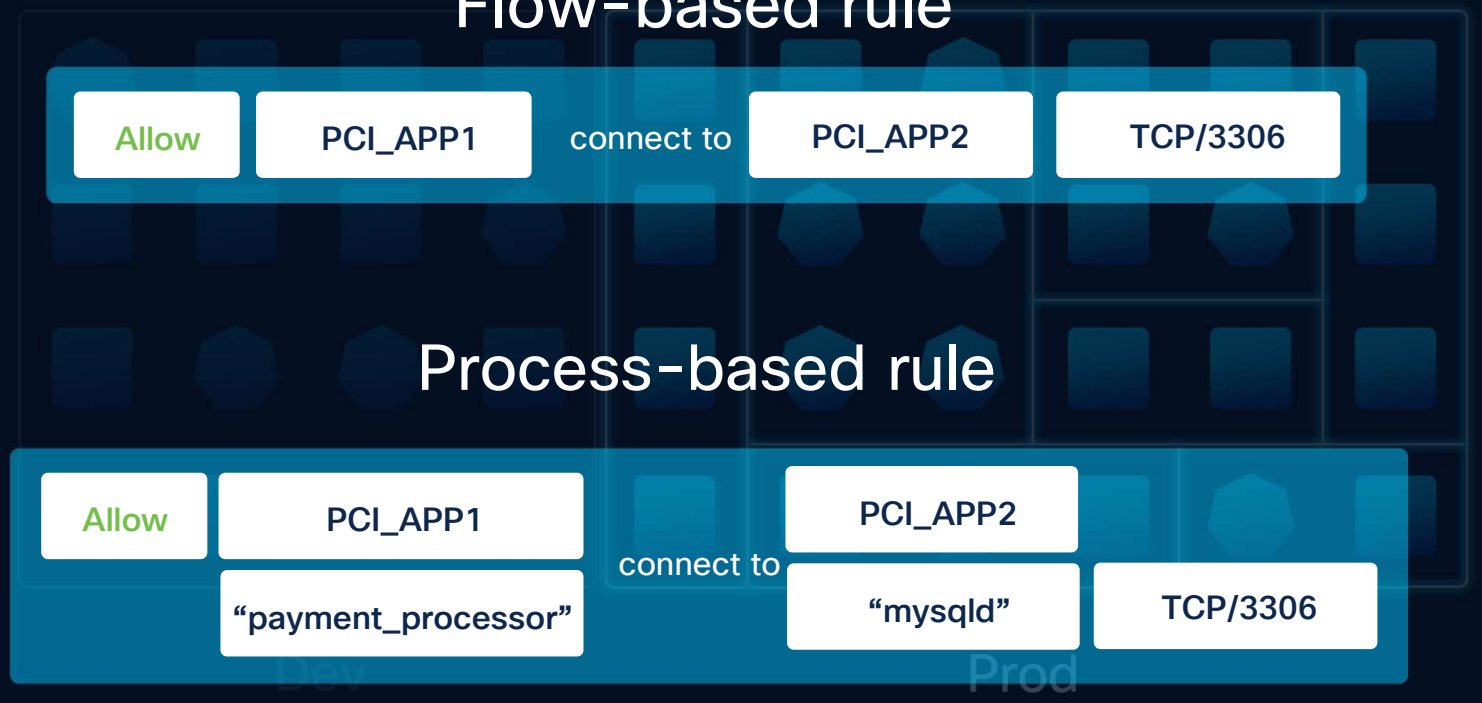
Dev

Prod

cisco

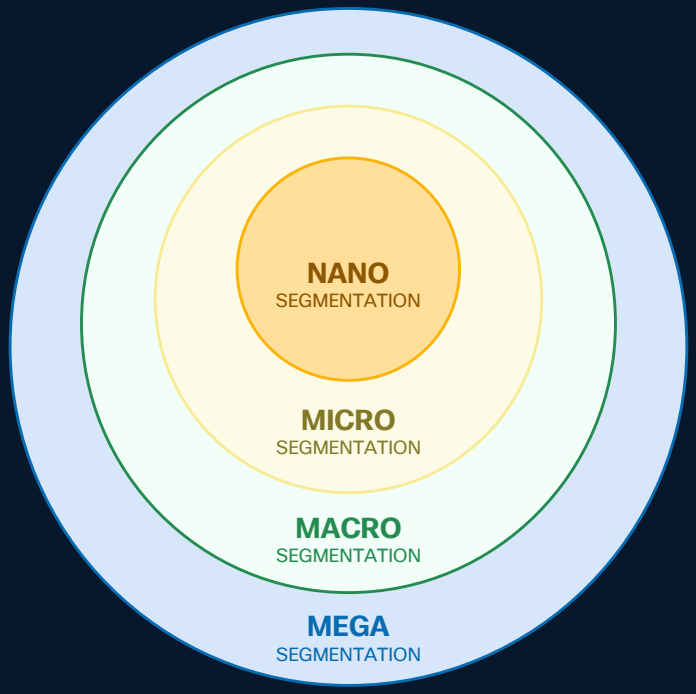
MACROSEGMENTATION

MICROSEGMENTATION



cisco

Importance of NANO Segmentation



Network Segmentation Spectrum

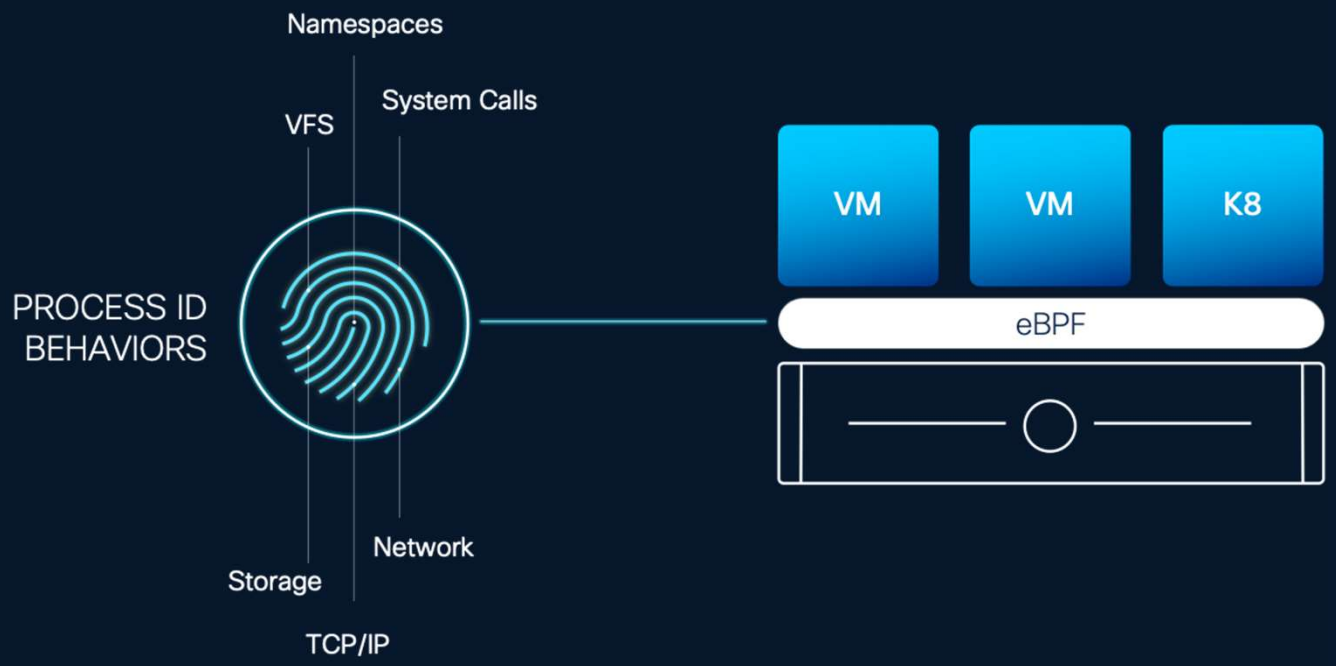
Mega Segmentation (The Perimeter)
- Broadest level of isolation (inside / outside boundary).
- Focuses on North-South traffic (Internet vs. Enterprise) and major domain separation (e.g., Data Center vs. Campus).

Macro Segmentation (The Zones)
- Logical grouping of assets (using VRFs, VLANs).
- Examples: Dev/Test/Prod, HR/Finance, EMEA/APAC).

Micro Segmentation (The Identity & Role)
- Granular isolation within a specific macro segment based on identity and function rather than IP addresses.
- Campus: Isolate users, devices, and IoT endpoints within the same VLAN (using Cisco TrustSec SGTs, VXLAN GPO)
- Data Center: Restricts East-West traffic between individual workloads or application tiers to prevent lateral movement (using Cisco ACI ESG/EPG, VLAN GPO)

Nano Segmentation (The Process)
- The highest level of precision; enforced at the OS, container, or process level.
- Focuses on individual service-to-service communication and API-level security within a single workload.

eBPF Provides Visibility Deep into the Workload



cisco

Summary

Secure Network

Any DC network that claims to be secure must support Mirco/Nano-segmentation

Ability to segment east-west traffic

Shrink the attack surface for better security

Auditing, compliance and conformance

cisco


CISCO