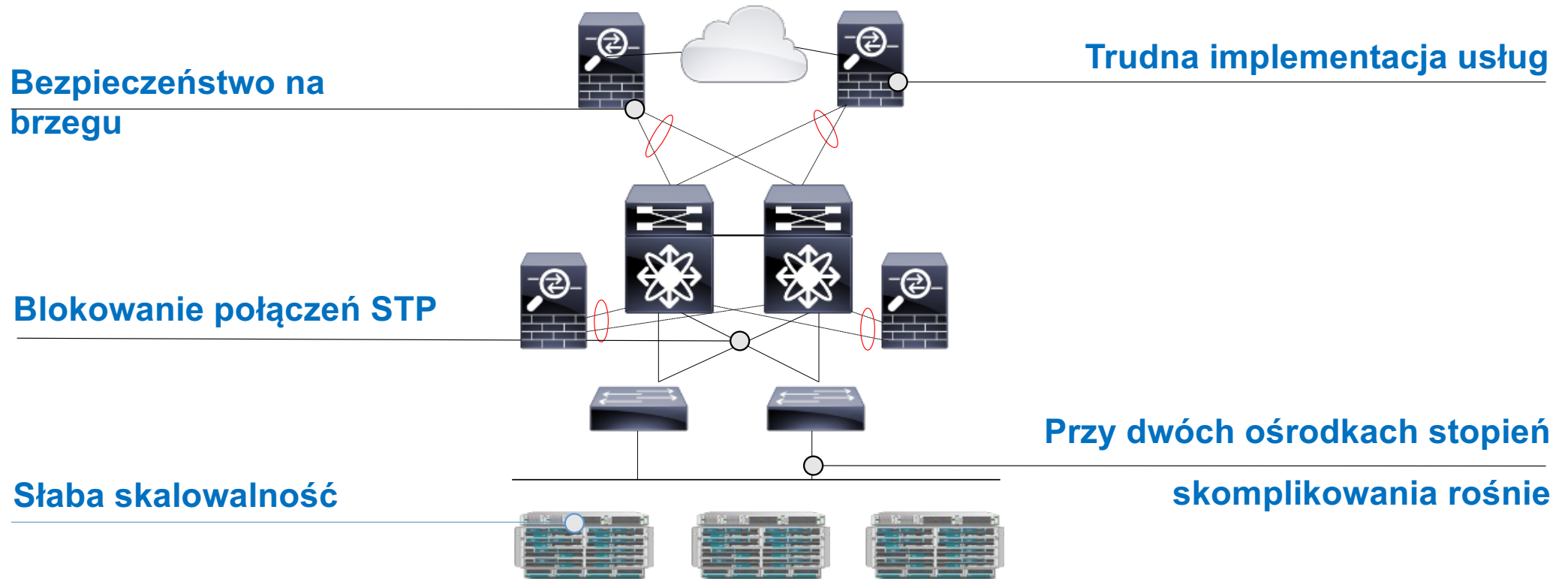


Cisco ACI i EVPN – nowoczesna sieć w Data Center, Cisco

Grzegorz Gondek
Konsultant Data Center
ggondek@cisco.com

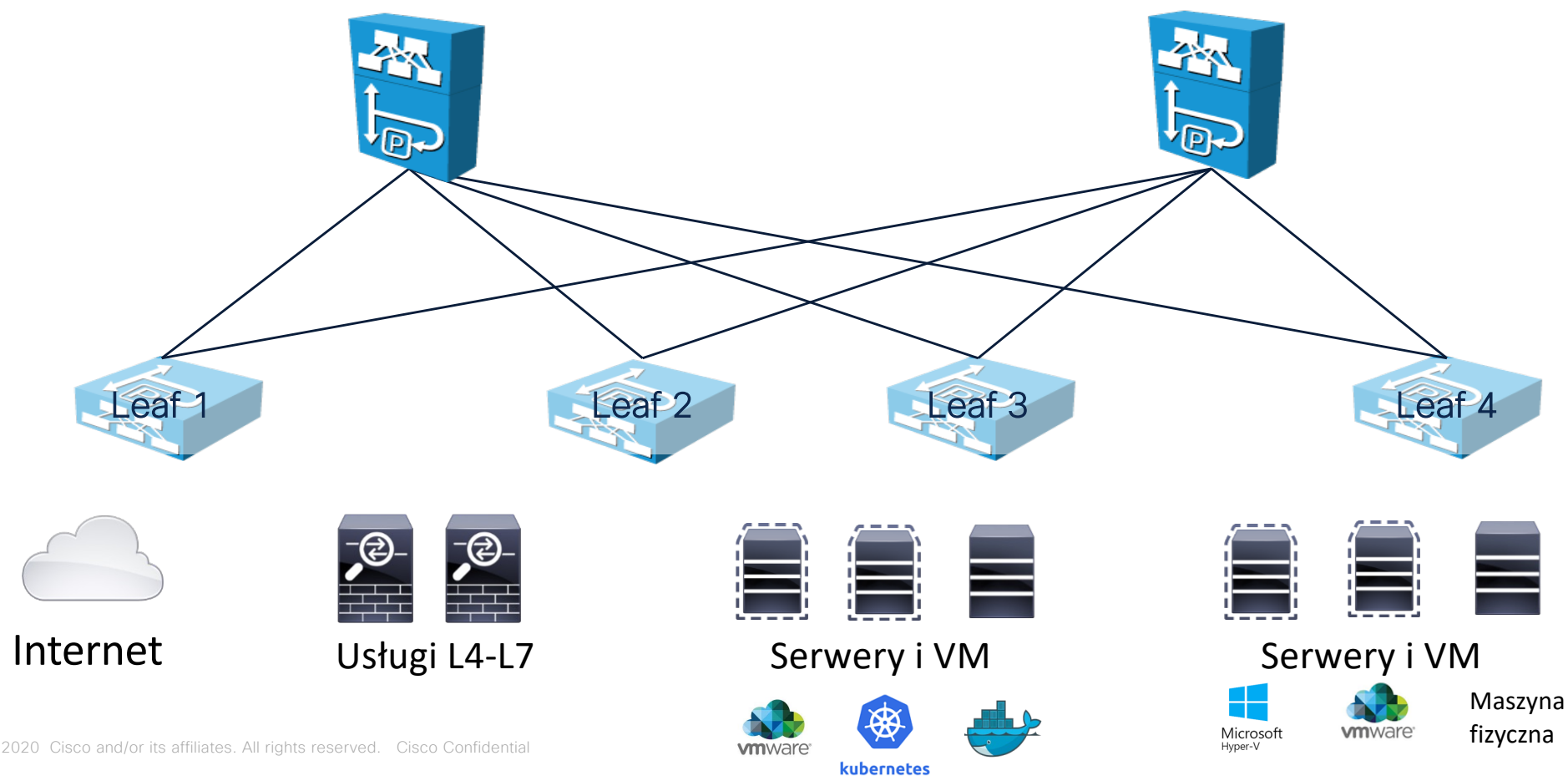
Jak buduje się sieci na potrzeby łączenia usług i serwerów?

Wady tradycyjnego modelu budowy infrastruktury



Architektura spine-leaf – model EVPN

Nieblokowna, wydajna i niezawodna – IP Fabric



1. Połączenia fizyczne



```
hostname spine201

interface loopback0
 ip address 10.10.10.201/32
 ip router ospf UNDERLAY area 0.0.0.0
```

```
router ospf UNDERLAY
 router-id 10.10.10.201
```

```
interface Ethernet1/1
 description Leaf101
 mtu 9192
 ip address 10.1.1.1/30
 ip ospf network point-to-point
 ip router ospf UNDERLAY area 0.0.0.0
 ip pim sparse-mode
```



```
hostname leaf101

interface loopback0
 ip address 10.10.10.101/32
 ip router ospf UNDERLAY area 0.0.0.0
```

```
router ospf UNDERLAY
 router-id 10.10.10.101
```

```
interface Ethernet1/1
 description Spine201 E1/1
 mtu 9192
 ip address 10.1.1.2/30
 ip ospf network point-to-point
 ip router ospf UNDERLAY area 0.0.0.0
 ip pim sparse-mode
```

```
interface Ethernet1/2 E1/1
 description Spine202
 mtu 9192
 ip address 10.1.1.6/30
 ip ospf network point-to-point
 ip router ospf UNDERLAY area 0.0.0.0
 ip pim sparse-mode
```

```
hostname spine202

interface loopback0
 ip address 10.10.10.202/32
 ip router ospf UNDERLAY area 0.0.0.0
```

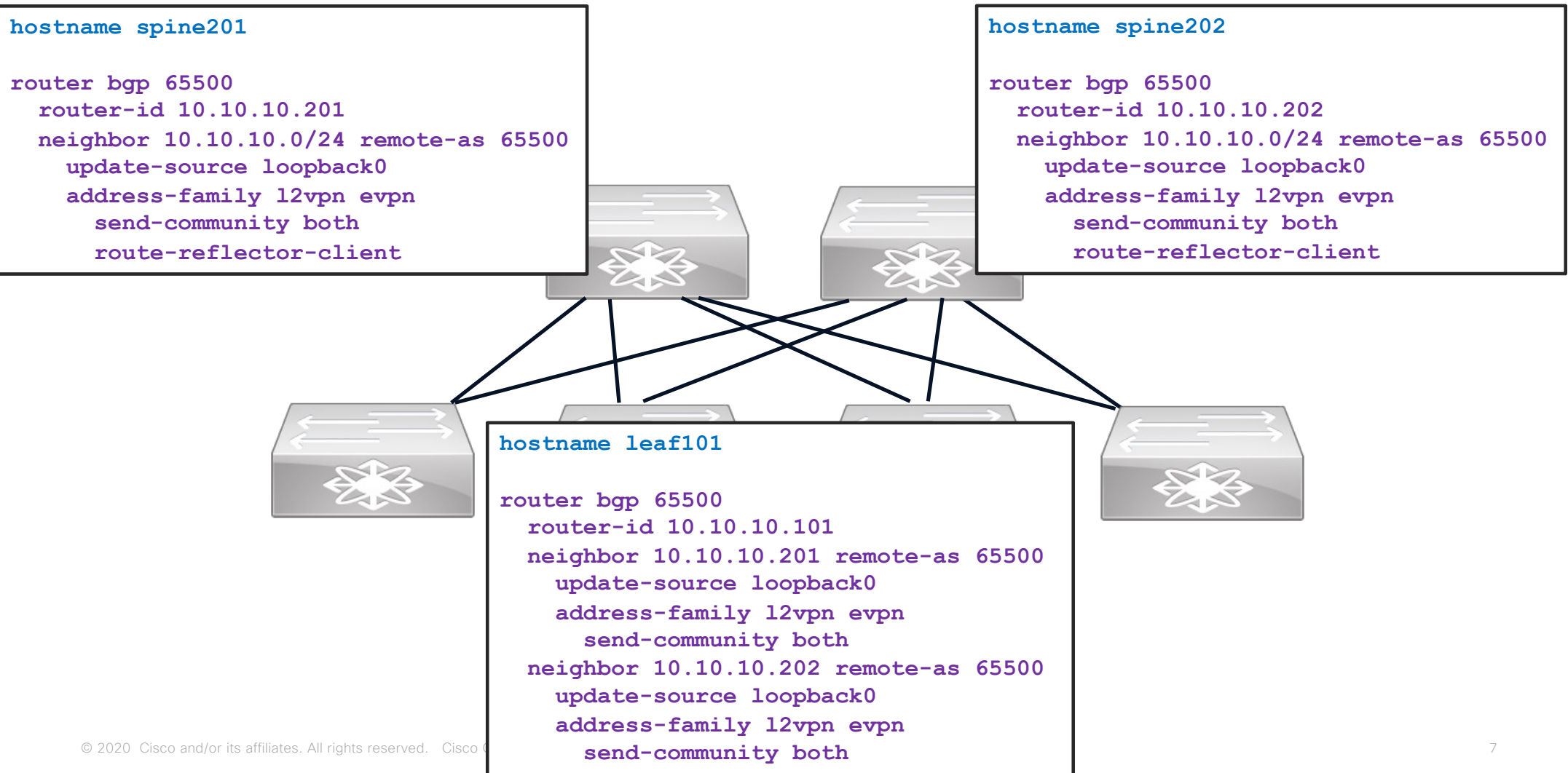
```
router ospf UNDERLAY
 router-id 10.10.10.202
```

```
interface Ethernet1/1
 description Leaf101
 mtu 9192
 ip address 10.1.1.5/30
 ip ospf network point-to-point
 ip router ospf UNDERLAY area 0.0.0.0
 ip pim sparse-mode
```

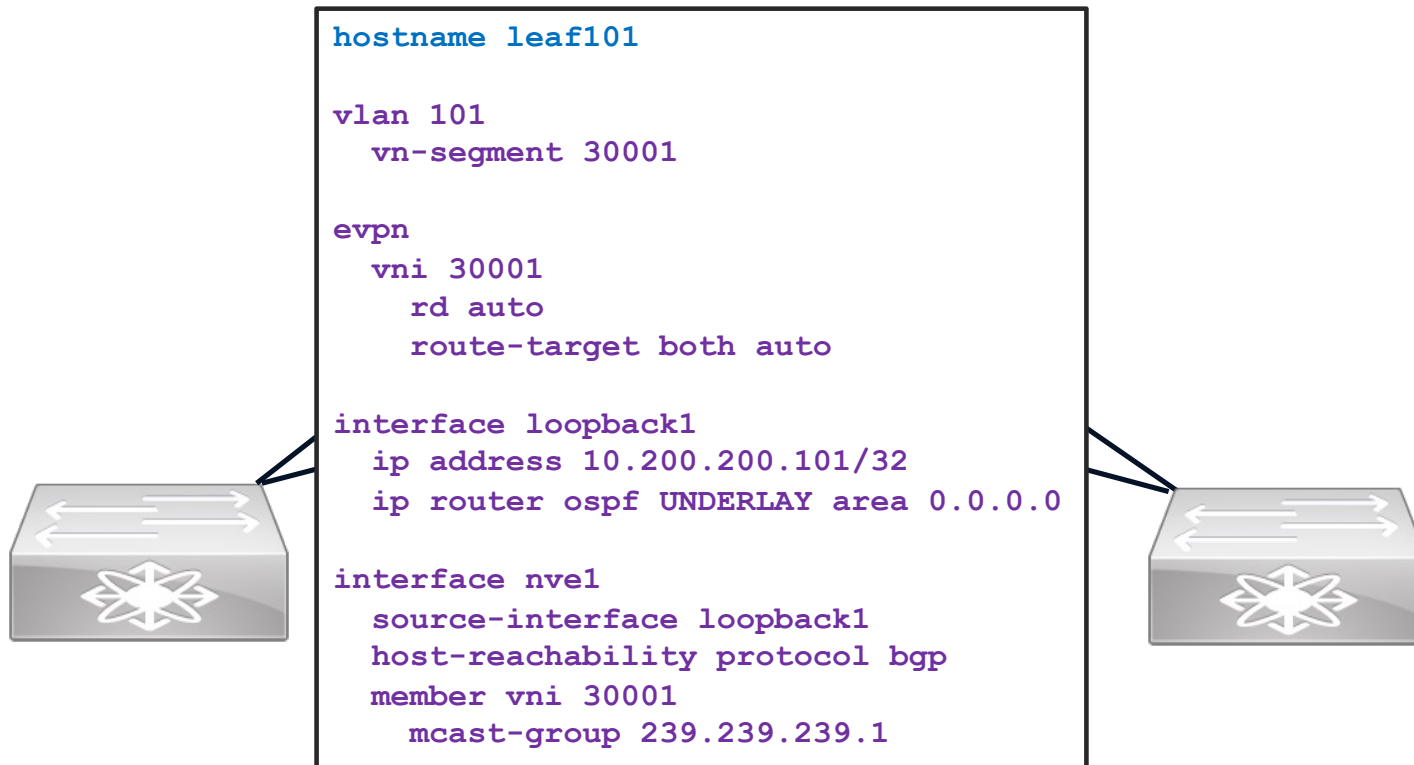




3. Control-Plane MP-BGP



4. Tunele VXLAN L2

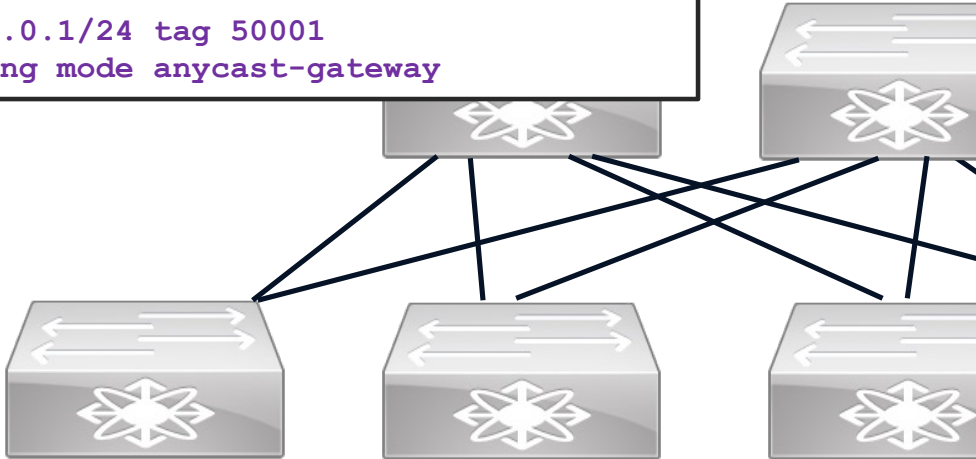


5. Brama domyślna i L3



```
! Na każdym Leaf
fabric forwarding anycast-gateway-mac 0002.0002.0002

interface Vlan101
  mtu 9192
  vrf member VRF-A
  ip address 20.0.0.1/24 tag 50001
  fabric forwarding mode anycast-gateway
```



```
hostname leaf101

vrf context VRF-A
  vni 50001
  rd auto
  address-family ipv4 unicast
    route-target both auto
    route-target both auto evpn

interface Vlan5001
  mtu 9192
  vrf member VRF-A
  ip forward
  no ip redirects

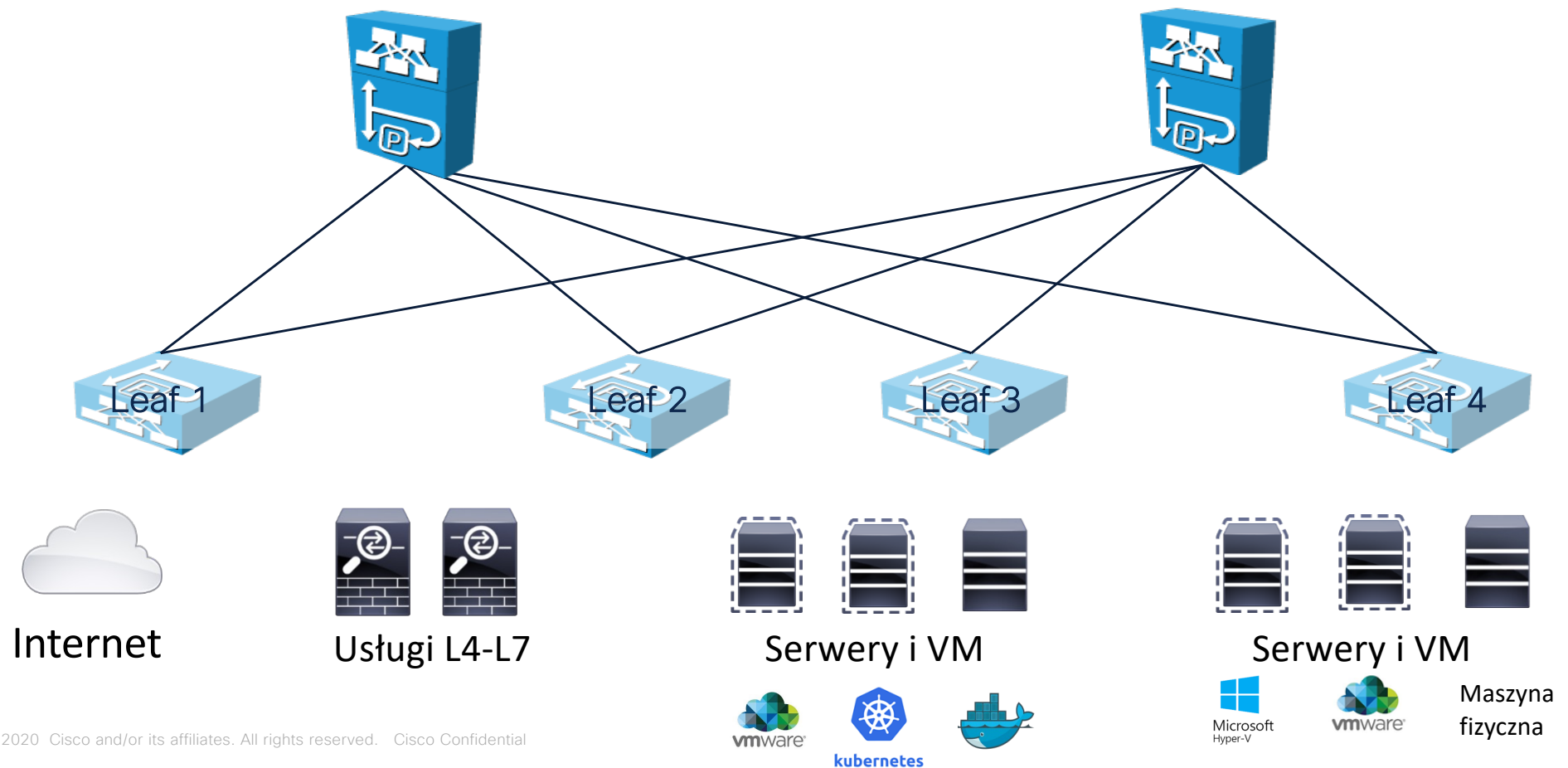
interface nve1
  member vni 50001 associate-vrf

router bgp 65500
  vrf VRF-A
    address-family ipv4 unicast
      advertise l2vpn evpn
      redistribute direct route-map TAG

route-map TAG permit 10
  match tag 50001
```

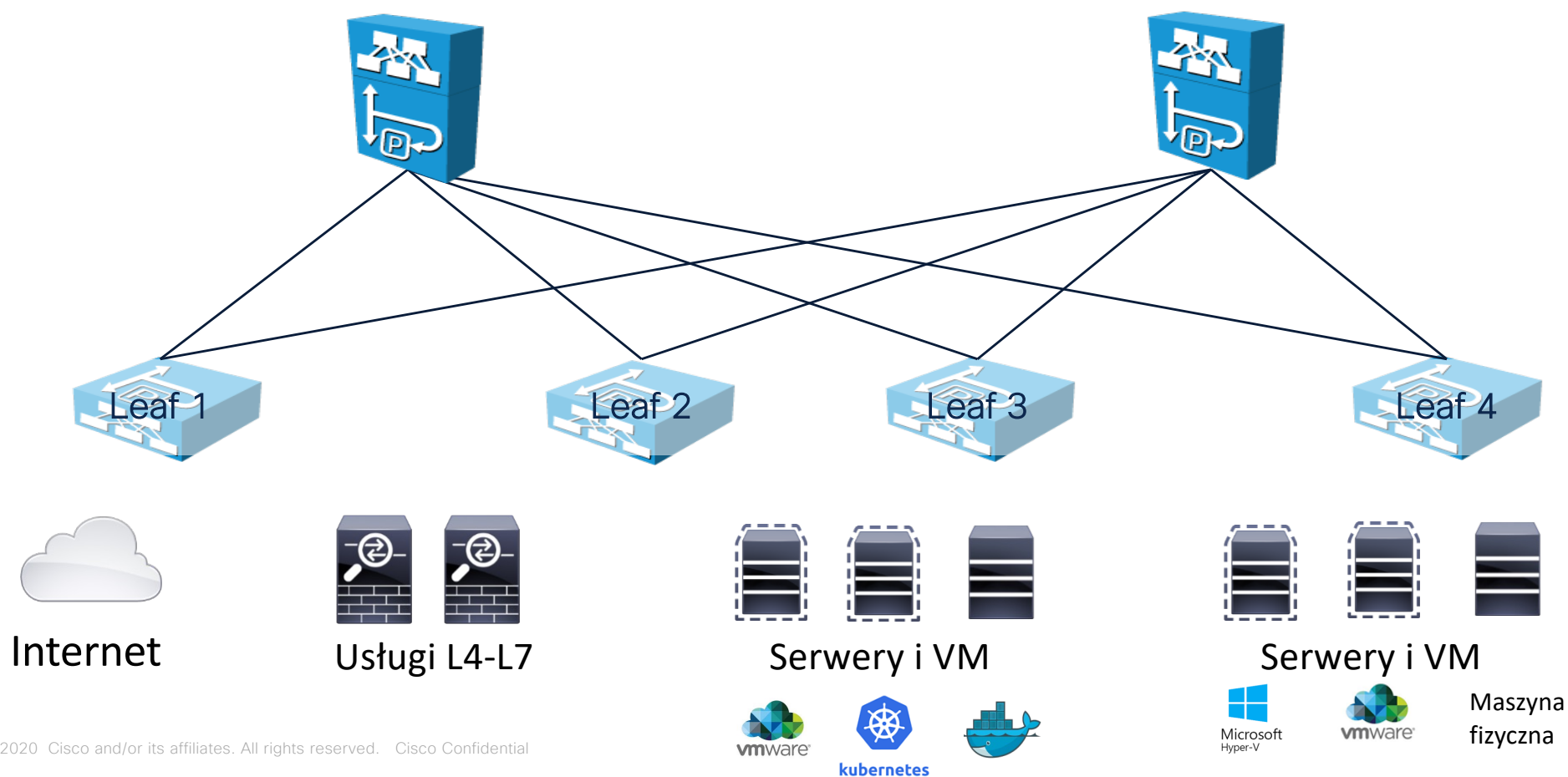
Architektura leaf-spine – model ACI

Kontroler zarządza kompletną infrastrukturą



Architektura spine-leaf – model ACI

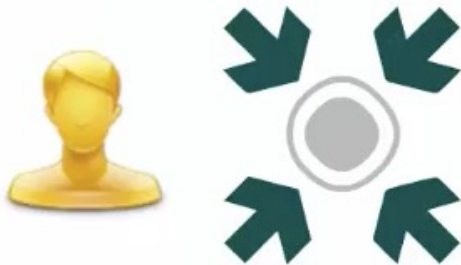
Kontroler zarządza kompletną infrastrukturą



Cisco Application Centric Infrastructure



Centralized Management



Embedded Security

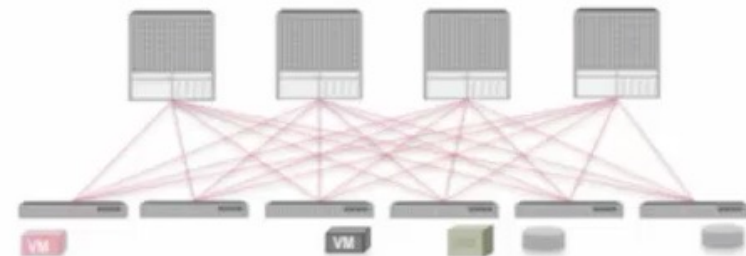


Lower
TCO

Health Monitoring

A screenshot of a health monitoring dashboard showing various system components and their status. The components include: CPU, Memory, Network, Storage, and System. Each component has a status bar (green for good, red for bad) and a list of metrics.

Deploy apps faster



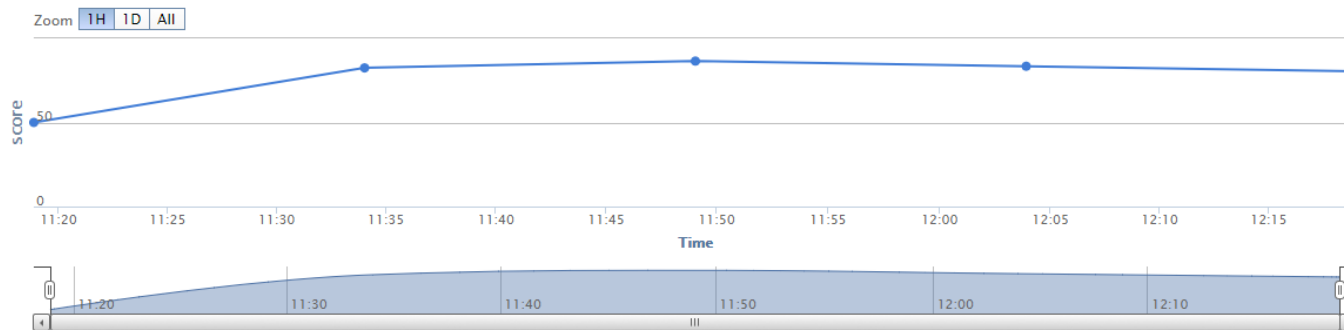
Konfiguracja, monitoring, troubleshooting



admin    

System Health

89



Fault Counts By Domain

☐ Hide Acked Faults

☐ Hide Delegated Faults

				
SYSTEM WIDE	3	29	10	517
Access	0	14	0	9
External	0	4	0	0
Framework	0	0	0	0
Infra	3	11	0	508
Management	0	0	2	0
Security	0	0	0	0
Tenant	0	0	8	0

Nodes With Health ≤ 99

99 

Name	POD ID	Type	Health Score
Leaf1	1	leaf	90
Leaf2	1	leaf	90
Spine1	1	spine	90
Spine2	1	spine	90

Fault Counts By Type

☐ Hide Acked Faults

☐ Hide Delegated Faults

				
Communicati...	0	14	0	0
Config	0	4	10	14
Environmental	0	4	0	0
Operational	3	7	0	503

Tenants With Health ≤ 100

100 

Name	Health Score
common	100
Deweloperzy	100
DMZ1	100
DMZ2	100
infra	100
Marketing	100

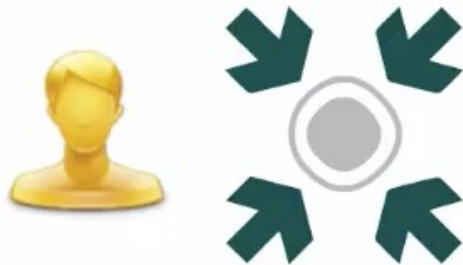
Controller Status

ID	Name	IP	Admin State	Operational State	Health State
1	apic1	10.0.0.1	In Service	Available	Fully Fit
2	apic2	10.0.0.2	In Service	Available	Fully Fit
3	apic3	10.0.0.3	In Service	Available	Fully Fit

Cisco Application Centric Infrastructure



Centralized Management



Embedded Security



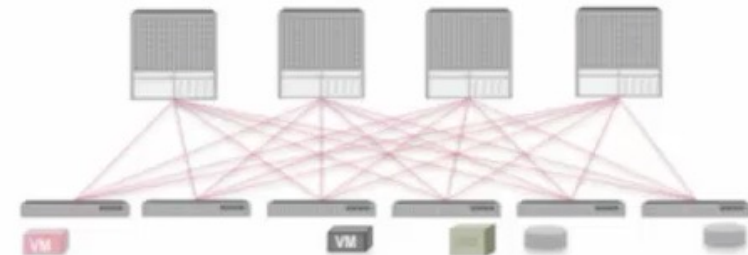
Lower
TCO

Health Monitoring

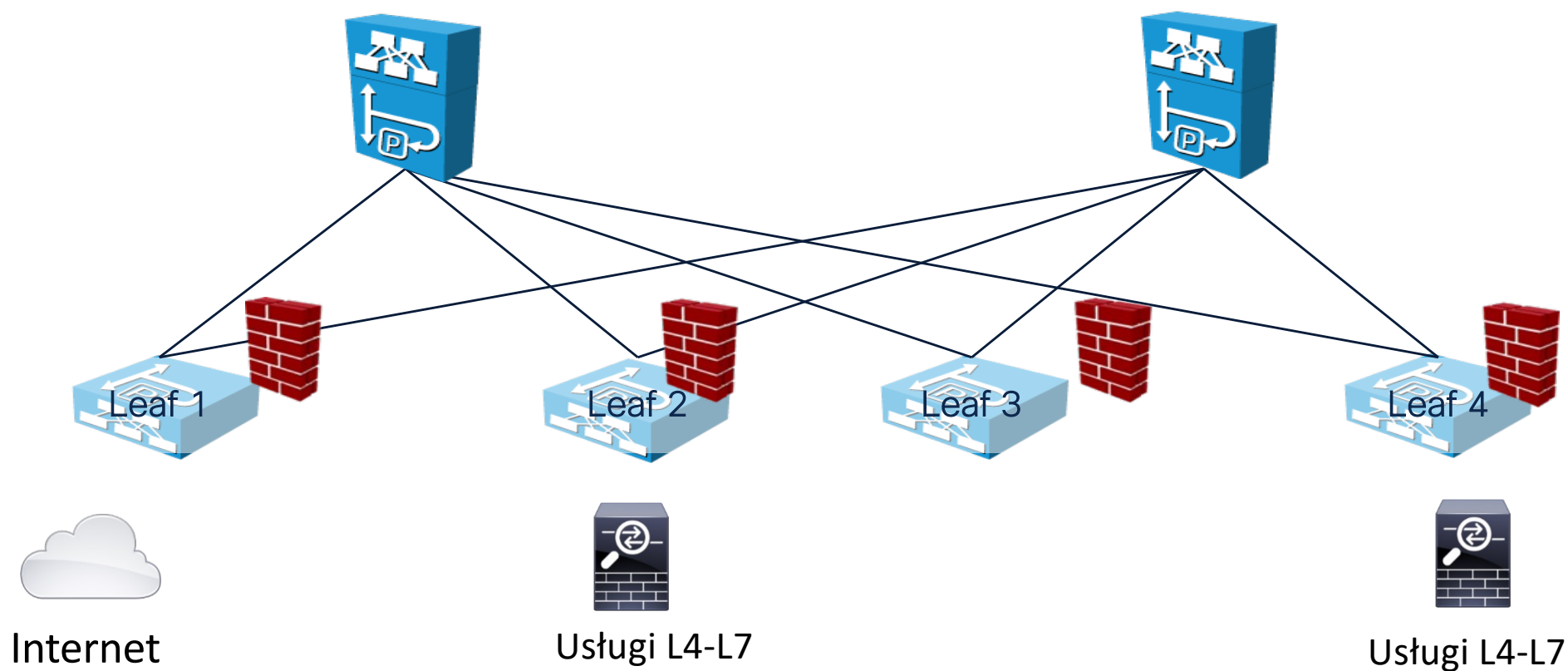
A screenshot of a health monitoring dashboard showing various system metrics and their status (up/down).

Component	Health	Details
System	Up	...
Network	Up	...
Storage	Up	...
Application	Up	...
Database	Up	...
Cache	Up	...
Queue	Up	...
Message	Up	...
Log	Up	...
Alert	Up	...
Configuration	Up	...
Policy	Up	...
Rule	Up	...
Service	Up	...
Endpoint	Up	...
Resource	Up	...
Capacity	Up	...
Performance	Up	...
Availability	Up	...
Reliability	Up	...
Security	Up	...
Compliance	Up	...
Logging	Up	...
Monitoring	Up	...
Alerting	Up	...
Reporting	Up	...
Configuration	Up	...
Policy	Up	...
Rule	Up	...
Service	Up	...
Endpoint	Up	...
Resource	Up	...
Capacity	Up	...
Performance	Up	...
Availability	Up	...
Reliability	Up	...
Security	Up	...
Compliance	Up	...
Logging	Up	...
Monitoring	Up	...
Alerting	Up	...
Reporting	Up	...

Deploy apps faster

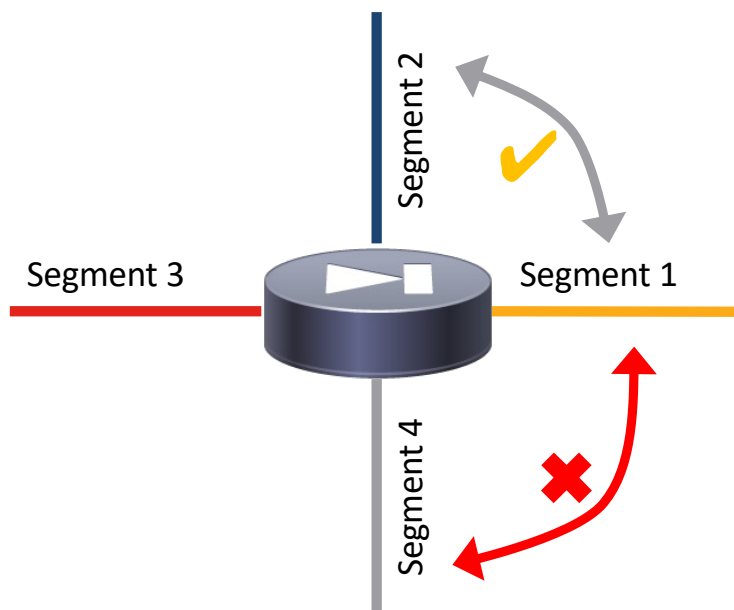


Bezpieczeństwo w ACI



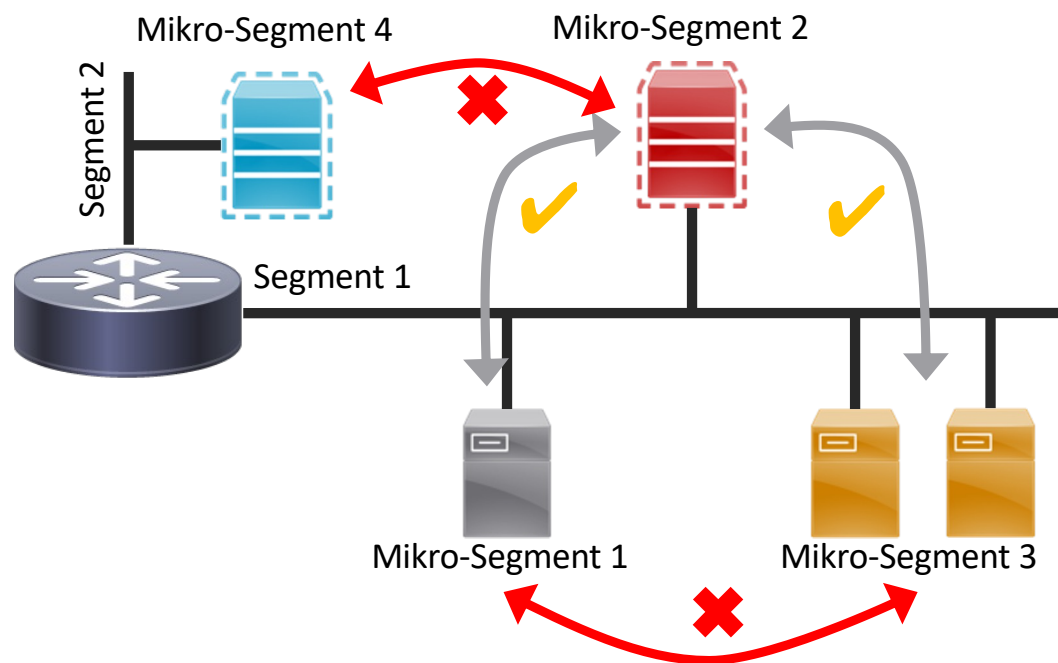
Bezpieczeństwo: Czym jest mikrosegmentacja?

Segmentacja



Segment = domena broadcast / VLAN / Podsieć

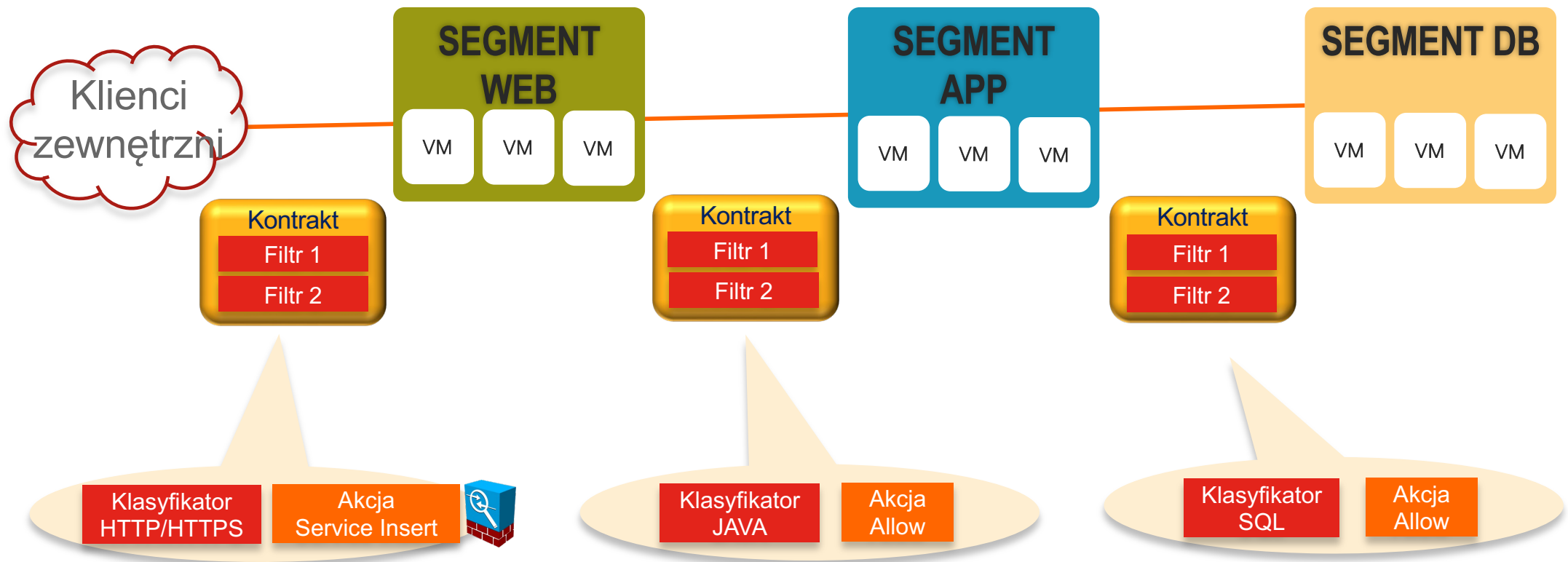
Mikrosegmentacja



Mikro-Segment = Urządzenie końcowe lub grupa urządzeń końcowych

Cisco ACI

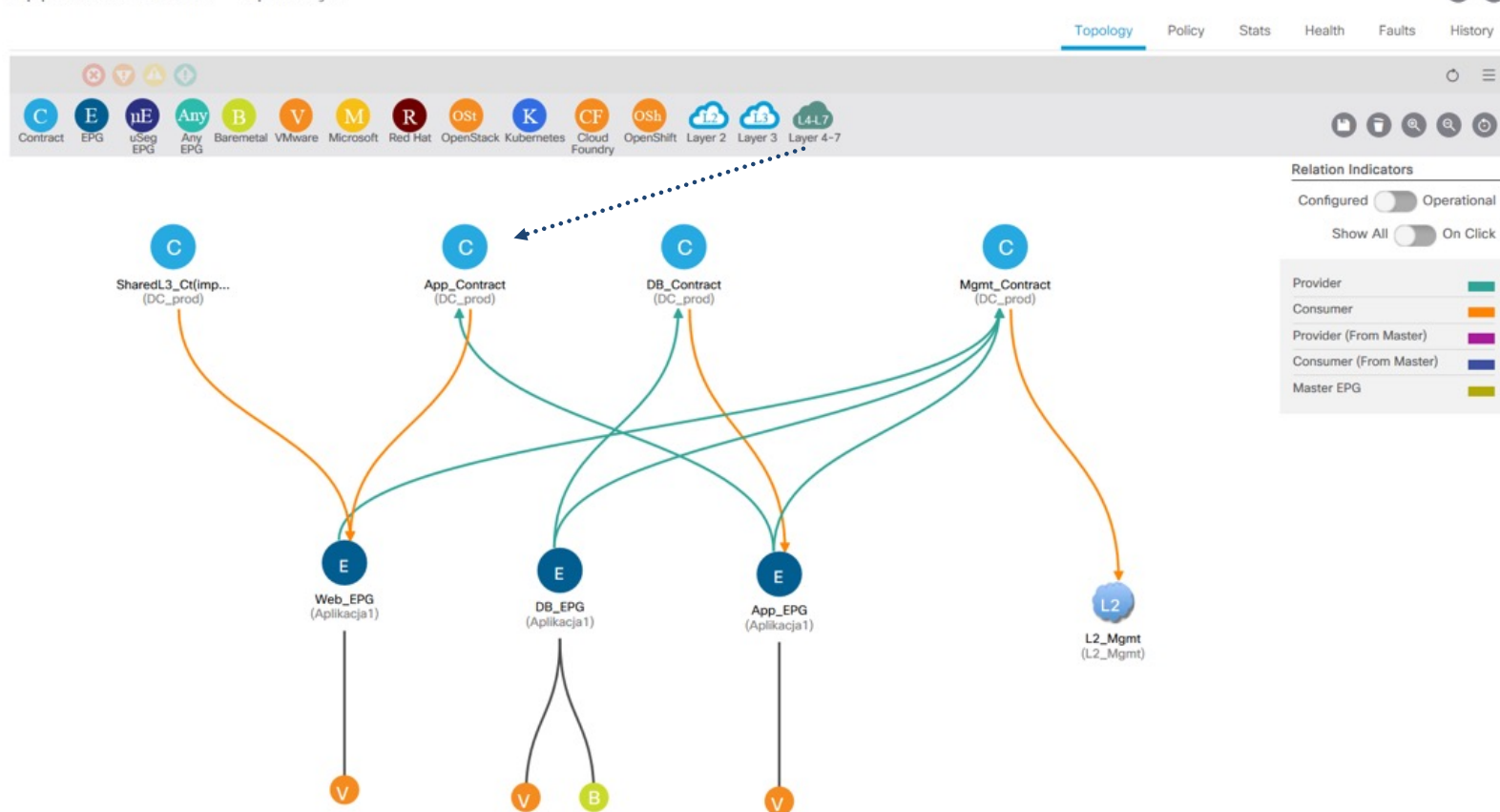
Profil aplikacji – polityki w akcji



EPG = End-Point Group-a = (u)Segment

Model logiczny aplikacji – segmenty i kontrakty

Application Profile – Aplikacja1



Zmiany polityk bezpieczeństwa wymagają jedynie zmian w kontraktach i/lub filtrach

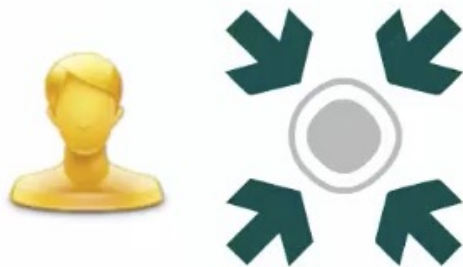
Propagacja zmian wszystkich powiązanych aplikacji i w całej sieci odbywa się automatycznie i natychmiast

Usunięcie filtru oznacza automatyczne usunięcie go ze wszystkich urządzeń. Znika problem utrzymania ACL na kilkudziesięciu urządzeniach

Co nie jest dozwolone jest zabronione

Cechy rozwiązania Cisco ACI

Centralized Management



Embedded Security



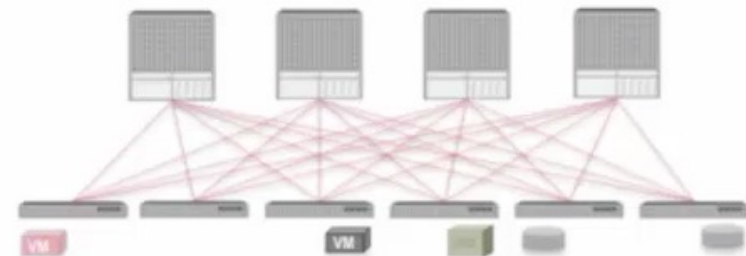
Lower
TCO

Health Monitoring



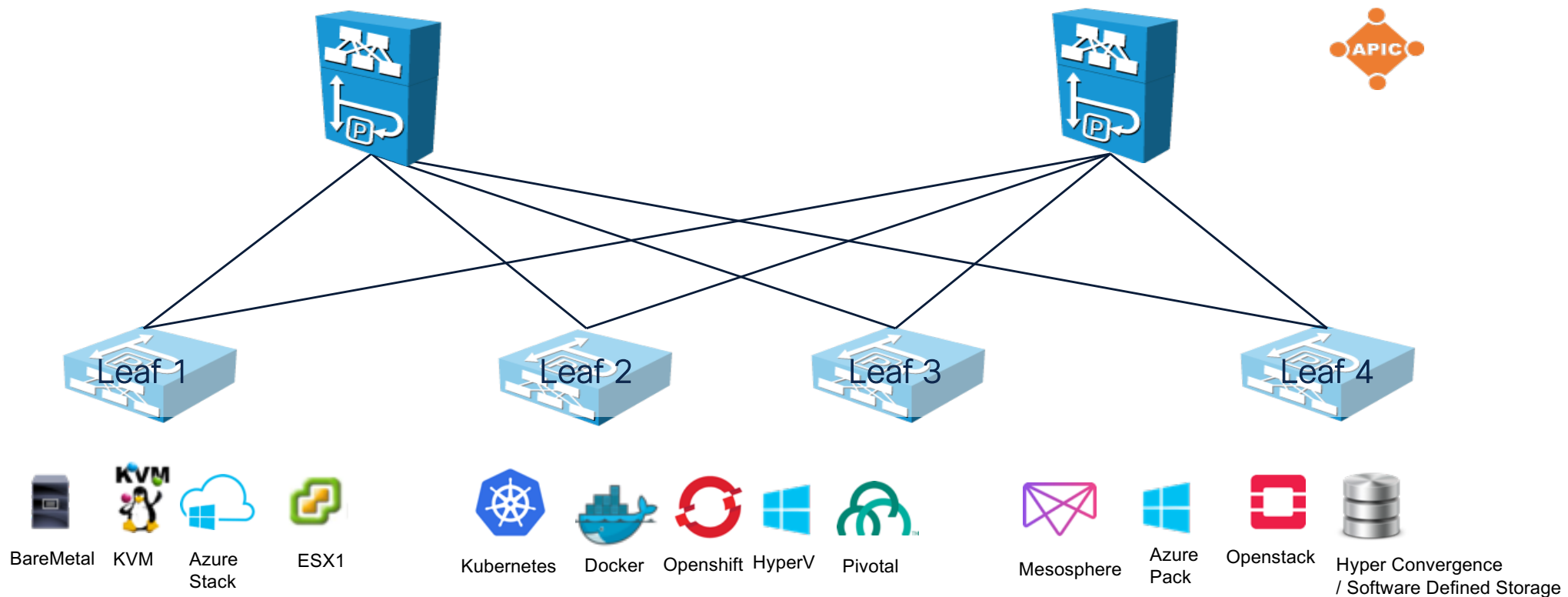
Component	Health	Details
System Health	OK	System is healthy
Network Health	OK	Network is healthy
Application Health	OK	Application is healthy
Security Health	OK	Security is healthy
Performance Health	OK	Performance is healthy

Deploy apps faster

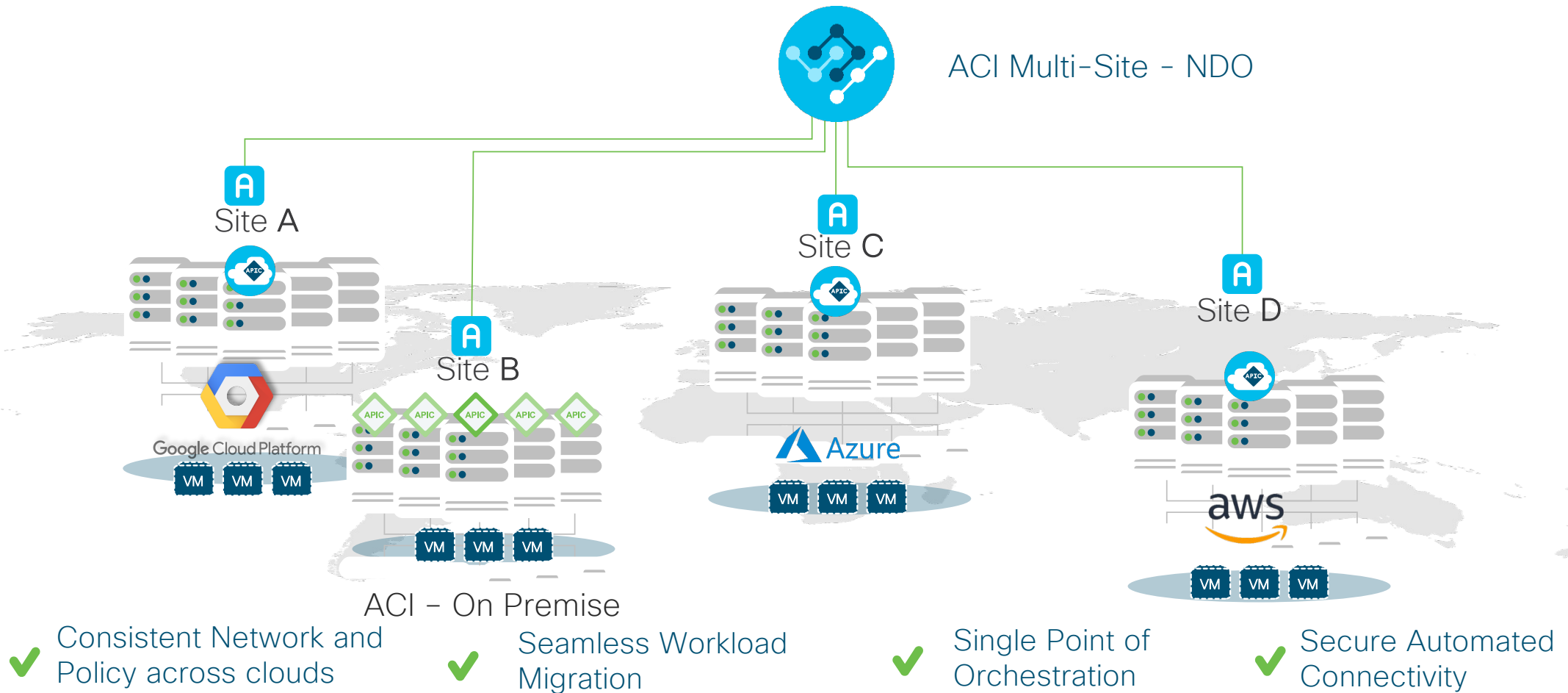


Owartość: Dołączanie systemów do fabryki Cisco ACI

Świat Data Center jest bardzo różnorodny. ACI w sposób spójny pozwoli go obsłużyć.



ACI Cloud/Multi-cloud



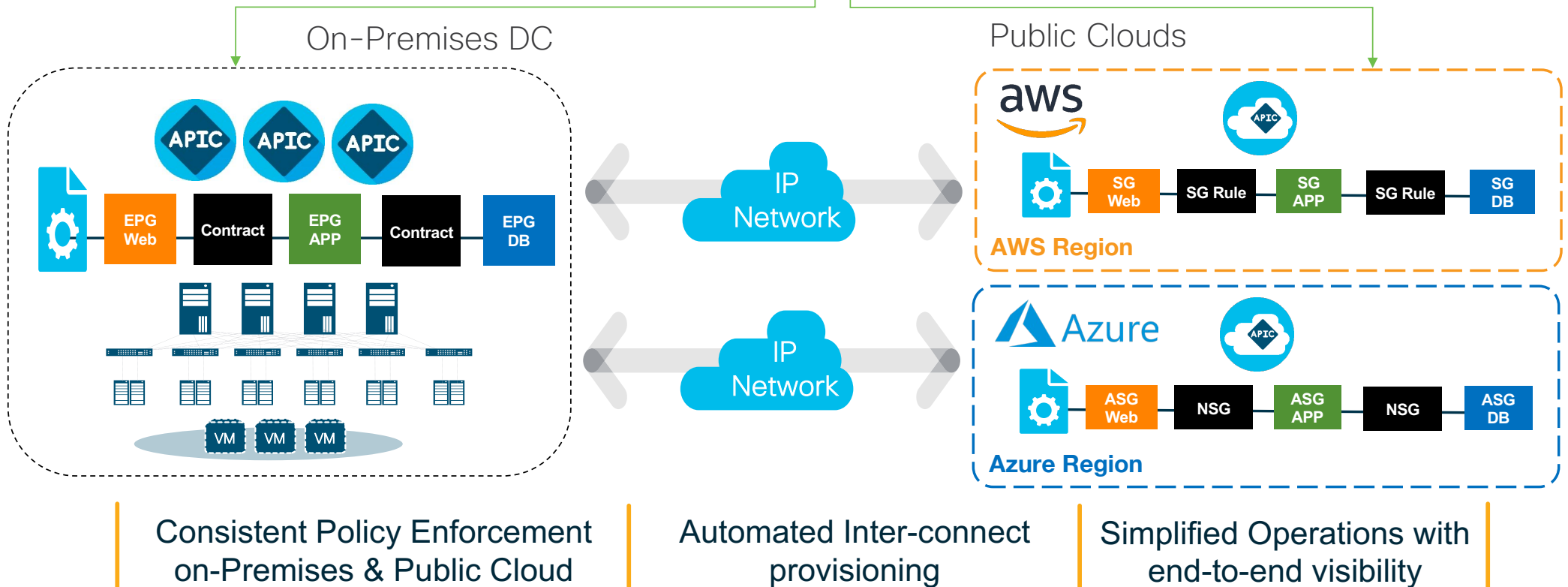
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

ACI Extension to Cloud

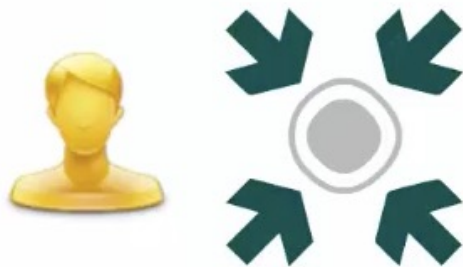


Multi-Site/NDO



Cechy rozwiązania Cisco ACI

Centralized Management



Embedded Security

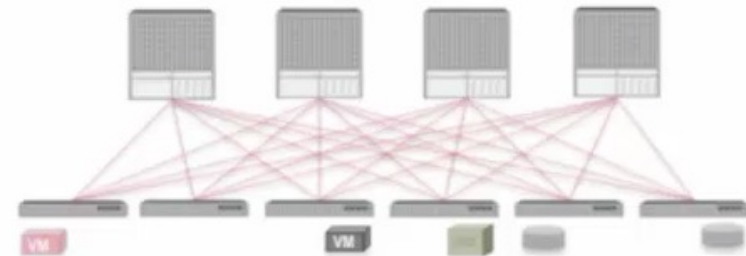


Lower
TCO

Health Monitoring



Deploy apps faster



Automatyzacja: jak powołać DC w 200ms?

APIC REST API

The screenshot displays the APIC REST API interface. The top navigation bar includes 'Runner', 'Import', and 'Builder' tabs. The 'Builder' tab is active, showing a 'Create Tenant' request. The request is a POST to the URL `https://10.62.0.183/api/node/mo/uni/tn-TenantX.xml`. The request body is in XML format, defining a tenant named 'TenantX' with various components like 'Router1', 'Web_BD', 'App_BD', 'DB_BD', 'L3Out_BD', and 'Mgmt_BD'. The interface also shows a 'History' panel on the left with a list of previous requests, including 'Login APIC', 'Create Tenant, 3 Tier App.L2/L3 Net - S...', 'Position Layout Srod1', 'Position Layout Srod2', 'Position Layout Srod3', 'Clone Tenant', and 'Position Layout 1'. The 'Response' panel is currently empty.

Filter

History Collections

All Me Team

ACI Lab 1 Initialize
7 requests

ACI Lab 2 Recreate L2-L3-VMM Config
28 requests

ACI Lab 3 Środowisko 1-3 ☆
13 requests

POST Login APIC

POST Create Tenant, 3 Tier App.L2/L3 Net - S...

POST Position Layout Srod1

POST Create Tenant, 3 Tier App.L2/L3 Net - S...

POST Position Layout Srod2

POST Create Tenant, 3 Tier App.L2/L3 Net - S...

POST Position Layout Srod3

POST Create Tenant

POST Position Layout

POST Clone Tenant

POST Position Layout 1

Create Tenant

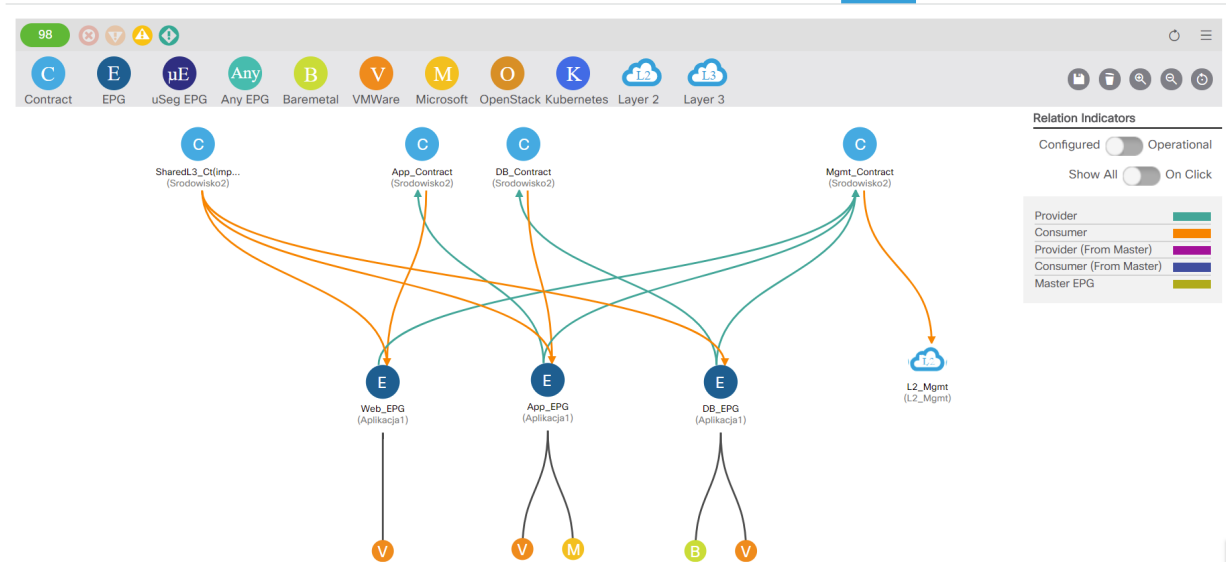
POST `https://10.62.0.183/api/node/mo/uni/tn-TenantX.xml`

Authorization Headers (1) Body Pre-request Script Tests

form-data x-www-form-urlencoded Application Profile - Aplikacja1

```
1 <fvTenant name="TenantX">
2   <fvCtx name='Router1' />
3   <fvBD name='Web_BD'>
4     <fvRsCtx tnFvCtxName='Router1' s
5     <fvSubnet ip='11.10.10.11/24' />
6   </fvBD>
7   <fvBD name='App_BD'>
8     <fvRsCtx tnFvCtxName='Router1' s
9     <fvSubnet ip='110.10.10.20/24' />
10  </fvBD>
11  <fvBD name='DB_BD'>
12    <fvRsCtx tnFvCtxName='Router1' s
13    <fvSubnet ip='128.11.10.10/24' />
14  </fvBD>
15  <fvBD name='L3Out_BD'>
16    <fvRsBDToOut tnL3extOutName='L3O
17    <fvSubnet ip='40.1.1.1/24' scope
18    <fvRsCtx tnFvCtxName='Router1' s
19  </fvBD>
20  <fvBD name='Mgmt_BD' unicastRoute=
21  <fvRsCtx tnFvCtxName='Router1' s
```

Response



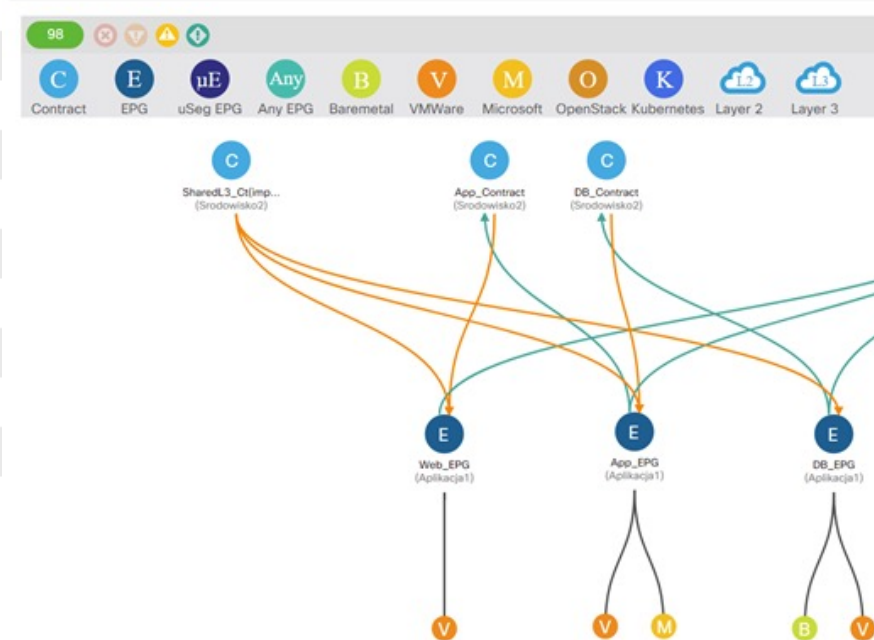
Automatyzacja: jak powołać DC w 200ms?

```
Health Score
100

QEdit - create_m...

1 import requests
2 import json
3
4 from config import url,user,pwd,tenant
5 requests.packages.urllib3.disable_warnings()
6
7 num_of_tenants = 10
8
9 auth = {'aaaUser':{'attributes':{'name':
10
11 session = requests.Session()
12
13 print('Logging to APIC...')
14 ret = session.post(url+'api/aaaLogin...')
15 if ret.ok:
16     print('Success')
17 else:
18     print('Login error: {}'.format(re
19
20 # prepare tenant data
21 # most have form {'<objectName>':{'at
22 # template to copy/paste {'':{'attrib
23 tenant = {'fvTenant':{'attributes':{'
24 vrf = {'fvCtx':{'attributes':{'name':
25 bd = {'fvBD':{'attributes':{'name': 'm
26 app = {'fvAp':{'attributes':{'name': '
27 # EPGs
28 web_epg = {'fvAEPg':{'attributes':{'na
29 app_epg = {'fvAEPg':{'attributes':{'na
30 db_epg = {'fvAEPg':{'attributes':{'na
```

Application Profile - Aplikacja1



al



```
Topology Policy Stats Health Faults History

98

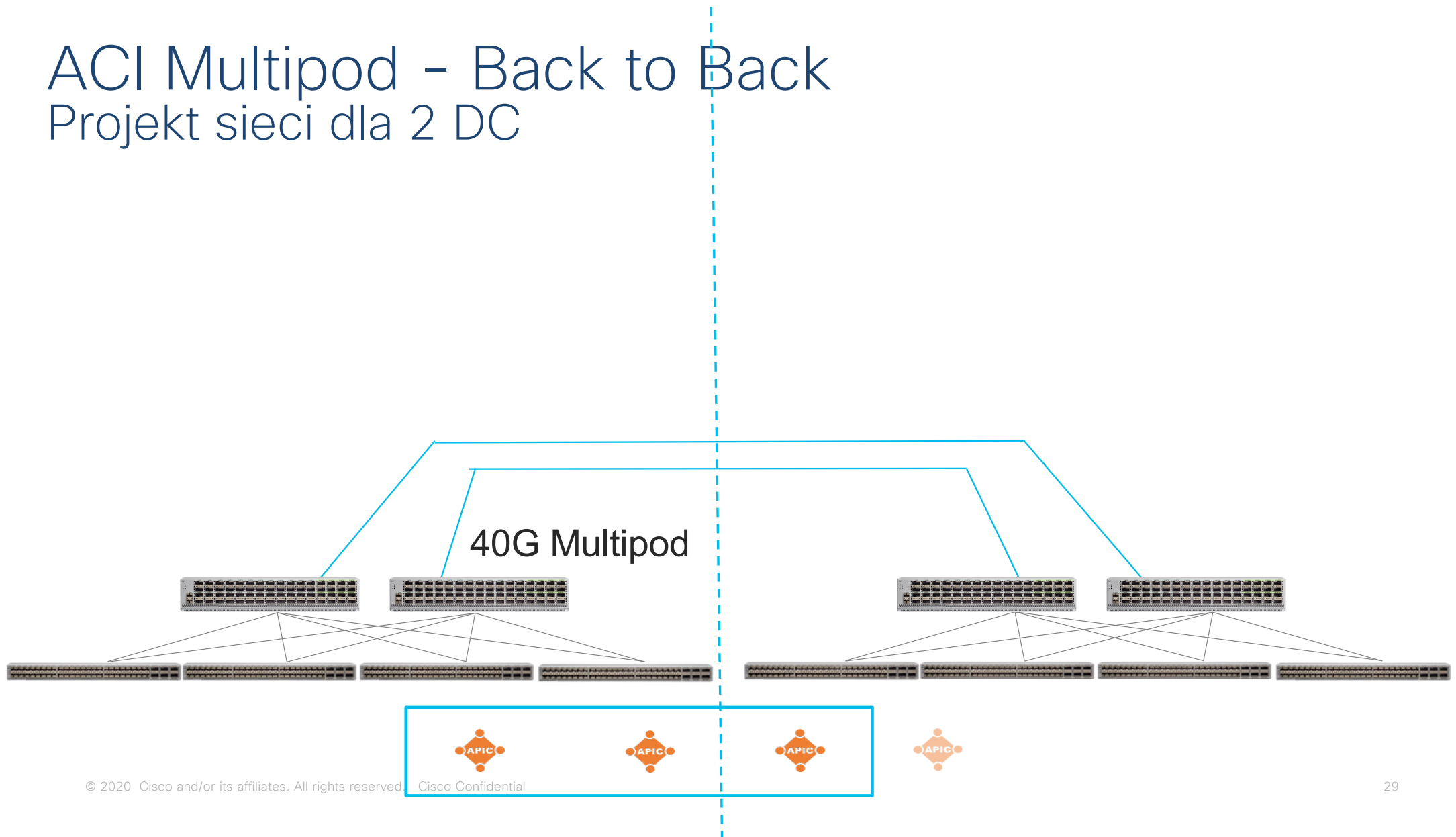
C E uE Any B V M O K Layer 2 Layer 3
Contract EPG uSeg EPG Any EPG Baremetal VMWare Microsoft OpenStack Kubernetes Layer 2 Layer 3

No. 1 SPECIAL KEYS

/data/user/0/com.hipipal.py3/files/bin/qpython-android5.sh "/storage/emulated/0/com.hipipal.pyplus/scripts3/.last_tmp.py" && exit
Logging to APIC...
Success
Pushing Tenant andrszul-TN001 to APIC...
Success
Pushing Tenant andrszul-TN002 to APIC...
Success
Pushing Tenant andrszul-TN003 to APIC...
Success
Pushing Tenant andrszul-TN004 to APIC...
Success
Pushing Tenant andrszul-TN005 to APIC...
Success
Pushing Tenant andrszul-TN006 to APIC...
Success
Pushing Tenant andrszul-TN007 to APIC...
Success
Pushing Tenant andrszul-TN008 to APIC...
Success
Pushing Tenant andrszul-TN009 to APIC...
Success
Pushing Tenant andrszul-TN010 to APIC...
Success
#[QPython] Press enter to exit
```

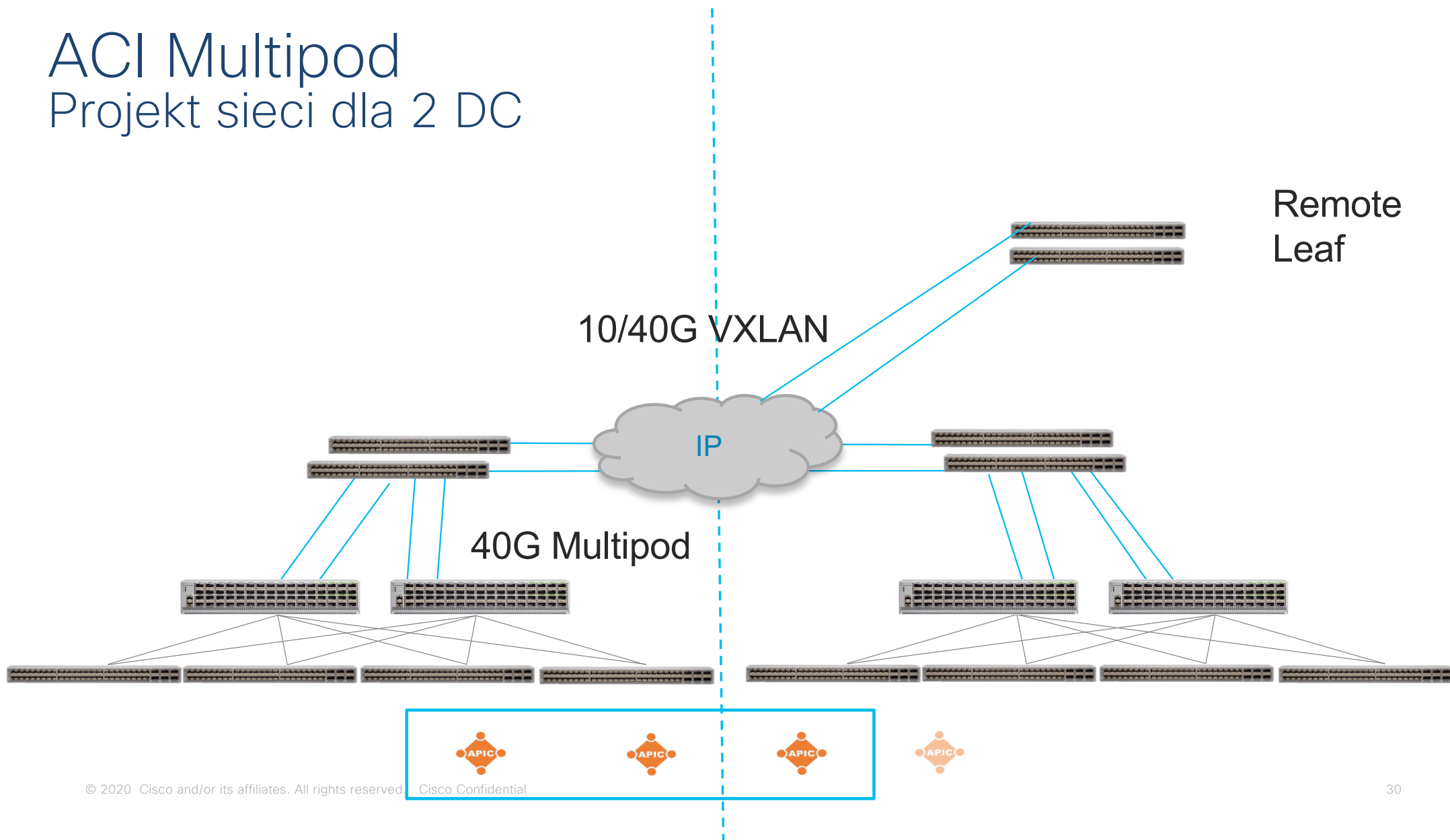
ACI Multipod – Back to Back

Projekt sieci dla 2 DC



ACI Multipod

Projekt sieci dla 2 DC



Platforma Nexus 9000

Cisco Nexus 9000

- Ponad 70 potężnych instalacji w Polsce EVPN/ACI
- Ponad 1500 sprzedanych urządzeń w Polsce
- Najczęściej sprzedawana i najbardziej rozwinięta linia przełączników Cisco Data Center
- Kompatybilność z przełącznikami poprzednich generacji (FEX)
- 3 modele wdrożenia, ten sam przełącznik, te same licencje – dowolność wyboru
- Świetne oprogramowanie do diagnostyki i zarządzania
- DCNM w cenie



Nexus 9300-FX Series



Nexus 93240YC-FX2
48p 10/25G SFP + 12p 40/100G QSFP



Nexus 93180YC-FX3
48p 10/25G SFP + 6p 40/100G QSFP



Nexus 93108TC-FX3P
48p 1/10GT + 6p 40/100G QSFP



Nexus C9336C-FX2-E
36p 40/100G

Dedykowana linia przełączników do Data Center

Działają z obraami NXOS oraz ACI

Wsparcie dla VXLAN, praca również w modelu EVPN

Elastyczna konfiguracja portów - 1/10/25/40/50/100 a także 400G

Wsparcie dla połączeń 25G powyżej 3m (RS FEC)

Możliwość wyboru kierunku chłodzenia przód/tył

Modularny system operacyjny

In Service Software Upgrade

(VPC vs VSS)

Zarządzanie za pomocą DCNM – z uwzględnieniem wirtualizacji

Pełna telemetria

Narzędzia diagnostyczne Day 2 Operations

Dodatkowo:

Szyfrowanie MACSEC/Cloudsec z pełną prędkością na portach 10G

32G FC support on all SFP ports

Wsparcie dla FEX-ów – zamiast stosów

Nexus 93240YC-FX2

1/10/25G Najlepszy przełącznik dla Data Center

- 48p - 1/10/25G + 12p 40/100G
- NX-OS lub ACI
- Redundantne chłodzenie i zasilanie
- Wybór kierunku chłodzenia
- Wspiera CloudSec i MACsec
- Telemetry
- Breakout



Nexus 93240YC-FX2

Beacon LED
Status LED
Environment LED

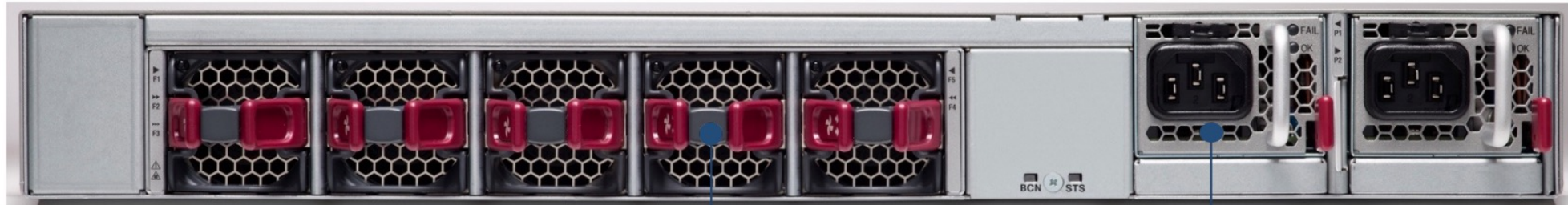
Console
Management
USB



48 x 1/10/25 GE SPF28

12 x 40/50/100-Gbps QSFP28

1.5 RU



5 (4+1) Fans

2 (1+1) PSU

1.5RU

Nexus 93180YC-FX3

1/10/25G Optimized NX-OS Switch

- 48p - 1G/10/25G SFP+
- 6p - 40/100G QSFP28
- NX-OS lub ACI
- Redundantne chłodzenie i zasilanie
- Wybór kierunku chłodzenia
- Telemetry



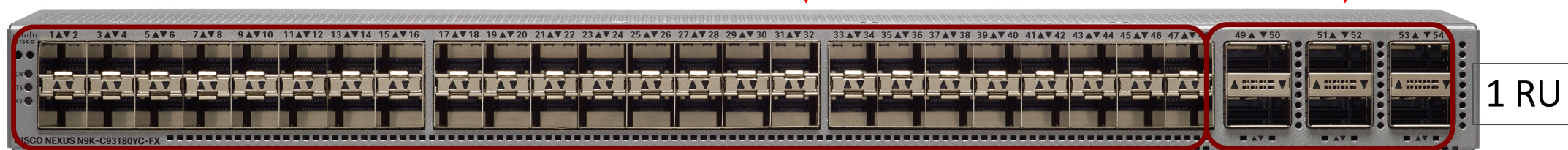
Nexus 93180YC-FX3

Nexus 93180YC-FX3

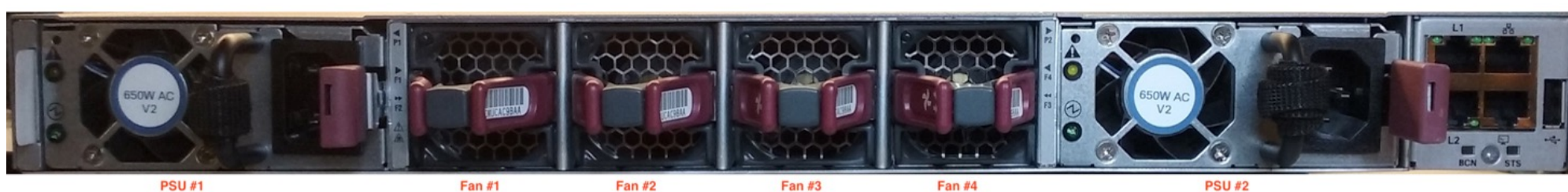
Szyfrowanie Cloudsec

48 x 1/10/25Gbps SFP28

6 x 40/100 Gbps QSFP28



1 RU



PSU #1

Fan #1

Fan #2

Fan #3

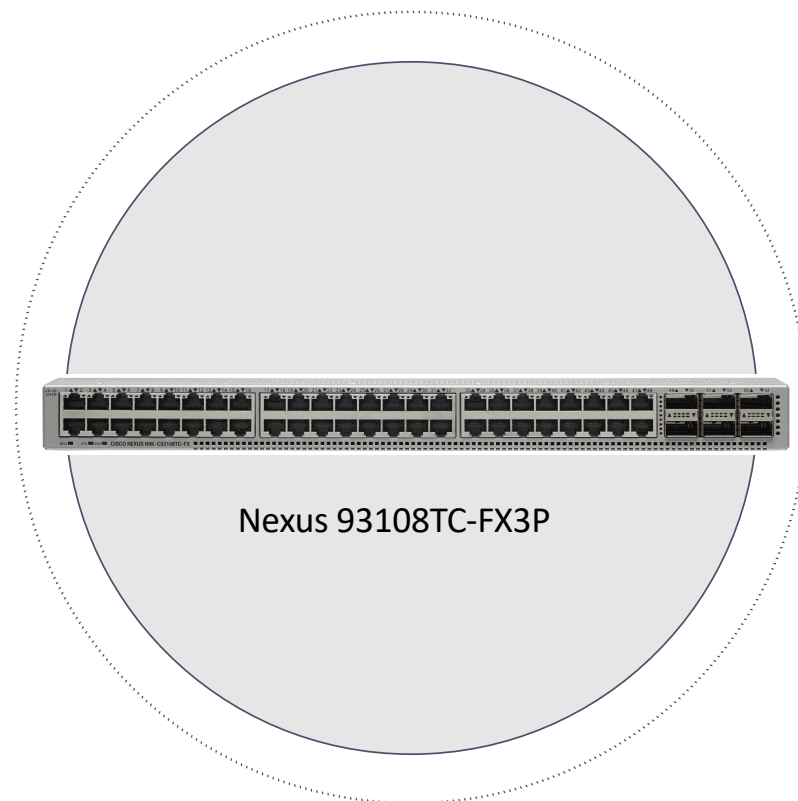
Fan #4

PSU #2

Nexus 93108TC-FX3P

1/10/25G Optimized NX-OS Switch

- 48p - 1G/10G RJ45
- 6p - 40/100G QSFP28
- NX-OS lub ACI
- Redundantne chłodzenie i zasilanie
- Wybór kierunku chłodzenia
- Telemetry



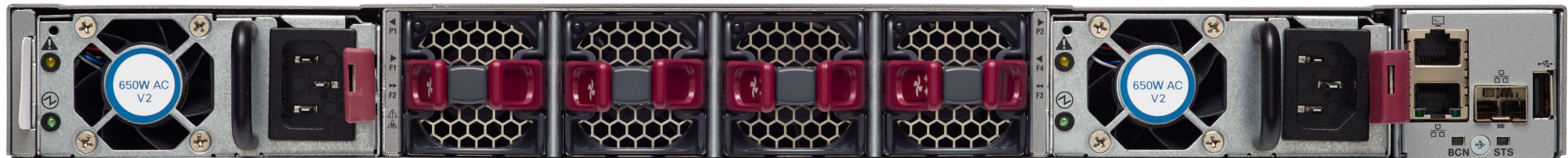
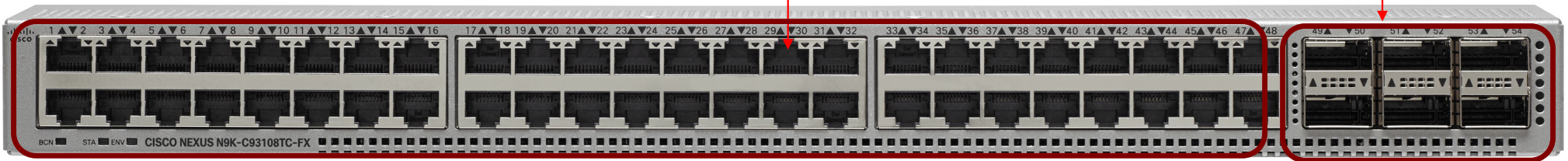
Nexus 93108TC-FX3P

Szyfrowanie Cloudsec

48 x 100M/1/10 Gbps T

6 x 40/100 Gbps QSFP28

1 RU



Nexus C9336C-FX2-E

40/100G Cost optimized NX-OS Switch

- 36p - 40/100G
 - NX-OS lub ACI
 - Redundantne chłodzenie i zasilanie
 - Wybór kierunku chłodzenia
 - 40MB bufory
 - Fiber Channel Capable (16G/32G)
 - Wspiera CloudSec i MACsec
 - Telemetry
 - Breakout



Nexus 9336C-FX2-E

MACSEC on all ports

36 x 40/100G

1 RU



Cisco Nexus 9000 Fixed Cloud Scale 1/10/25G Switches

Nexus 9300 FX2

96p 1/10GT + 12p 100G QSFP28
Nexus 93216TC-FX2



96p 25G SFP + 12p 100G QSFP28
Nexus 93360YC-FX2



48p 25G SFP + 12p 100G QSFP28
Nexus 93240YC-FX2

Nexus 9300 FX3

48p 1/10GT + 6p 100G QSFP28
Nexus 93108TC-FX3P



48p 25G SFP + 6p 40/100G QSFP
Nexus 93180YC-FX3



48p 100M/1GT + 4p 25G SFP + 2p 100G QSFP28
Nexus 9348GC-FXP



Nexus 9300 high density 400G switches



Nexus 9332D-GX2B

32p 400G
8p MACsec/CloudSec



Nexus 9348D-GX2A

48p 400G
4p MACsec/CloudSec



Nexus 9364D-GX2A

64p 400G
16p MACsec/CloudSec



Nexus 9316D-GX

16p 400G



Nexus 93600CD-GX

28p 100G + 8p 400G

Podsumowanie

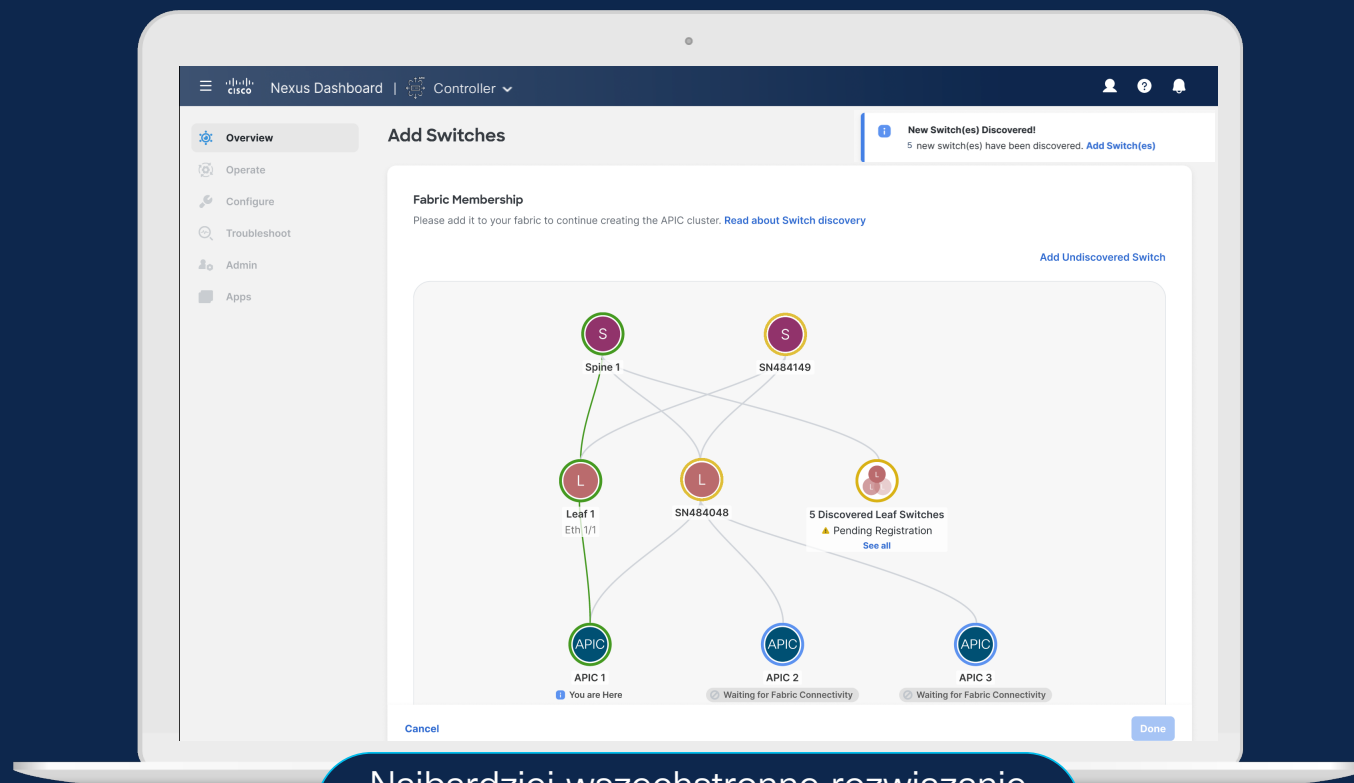
Cisco ACI

Centralne zarządzanie

Bezpieczeństwo

Automatyzacja

Nowy sposób konfiguracji



Najbardziej wszechstronne rozwiązanie
SDN



C97-3853695-00 © 2023 Cisco Systems, Inc., and/or its affiliates. All rights reserved. Cisco Confidential. For Channel Partner

¹ ACI Controller integrated to Nexus Dashboard Option in roadmap
² NDFC and ACI new look and feel planned for ND 3.1 and ACI 6.1.1 respectively

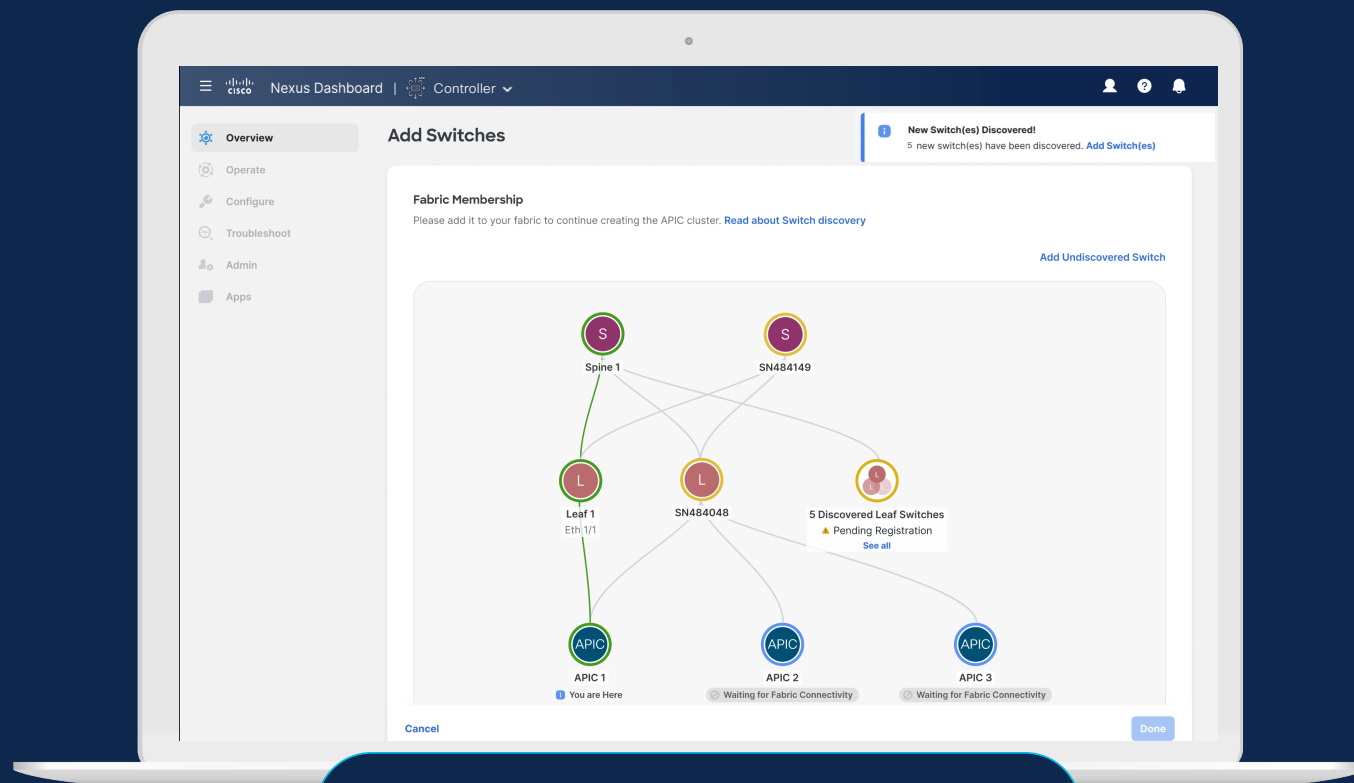
Cisco Nexus Dashboard – Controller

Centralne zarządzanie

Prosty, znany język konfiguracji

Brak mikrosegmentacji

Automatyzacja



Nowy interfejs, te same licencje



C97-3853695-00 © 2023 Cisco Systems, Inc., and/or its affiliates. All rights reserved. Cisco Confidential. For Channel Partner

¹ ACI Controller integrated to Nexus Dashboard Option in roadmap
² NDFC and ACI new look and feel planned for ND 3.1 and ACI 6.1.1 respectively