CERT-MZ
Maputo
Agosto 2018

TENDÊNCIAS

AS ACTUAIS MELHORES PRÁTICAS EM TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO PARA CENTROS DE DADOS ….SEM DESCURAR A SEGURANÇA

Paulo Machado
pmachado@net4sysops.com
+258 823500060

APLICAÇÕES E NEGÓCIO

- As emergentes tecnologias de IC
  - Deixaram de ser um centro de custos
  - Passaram a ser um catalizador do negócio
- Mudanças
  - Modelos de operação em “cloud”
  - Infraestrutura de conectividade baseada em SDN – “Software Defined Networking”

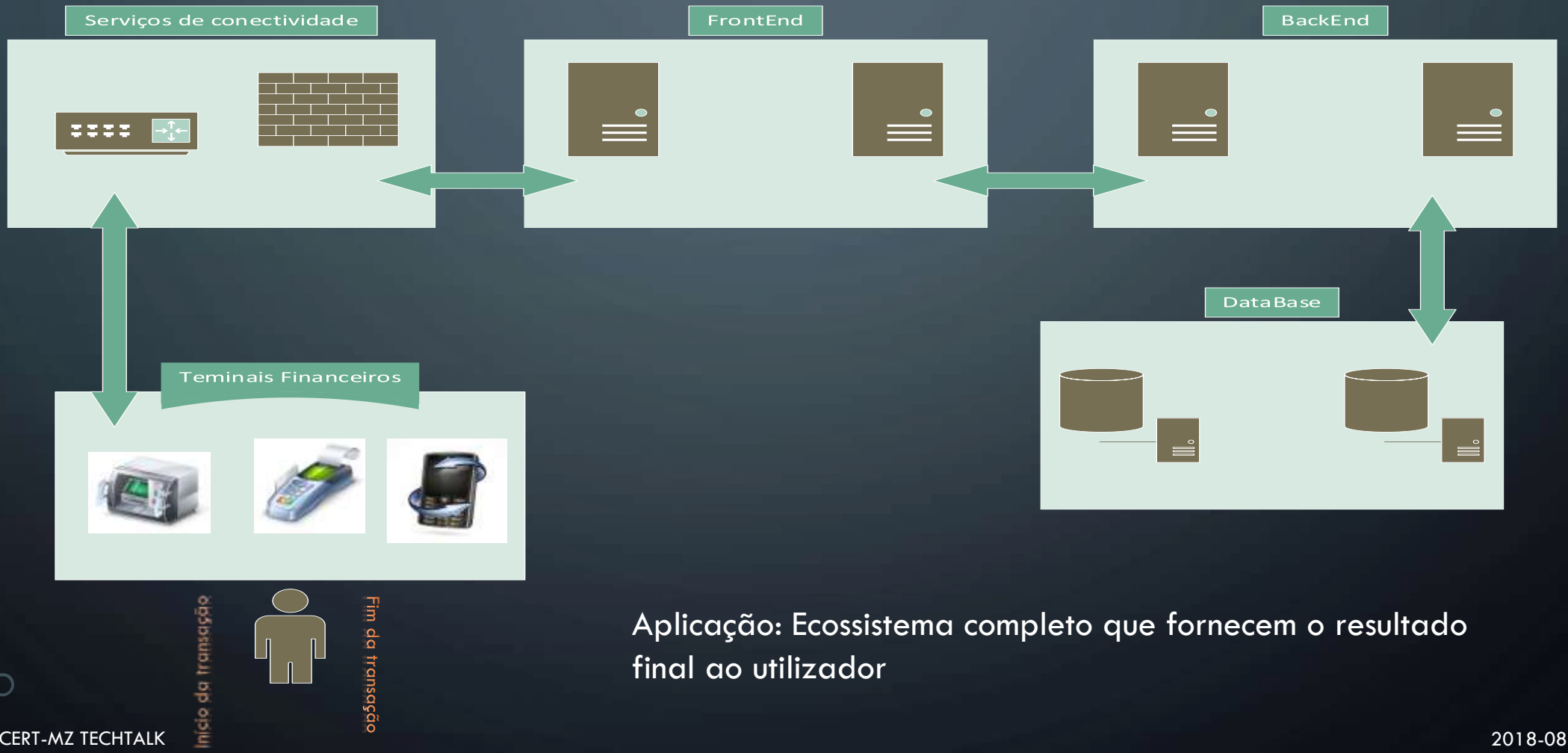
Aplicação é o foco primário

APLICAÇÕES

- Aplicações influenciam o negócio
  - Portais web
  - Sistemas de gestão de recursos financeiros
  - Sistemas de gestão de recursos humanos
  - Sistemas de gestão de recursos técnicos
- Aplicações são ecossistemas de componentes interligados
  - Físicos
  - Virtuais
  - Antigos
  - Novos

Objectivo: Promoção do valor do negócio

APLICAÇÕES

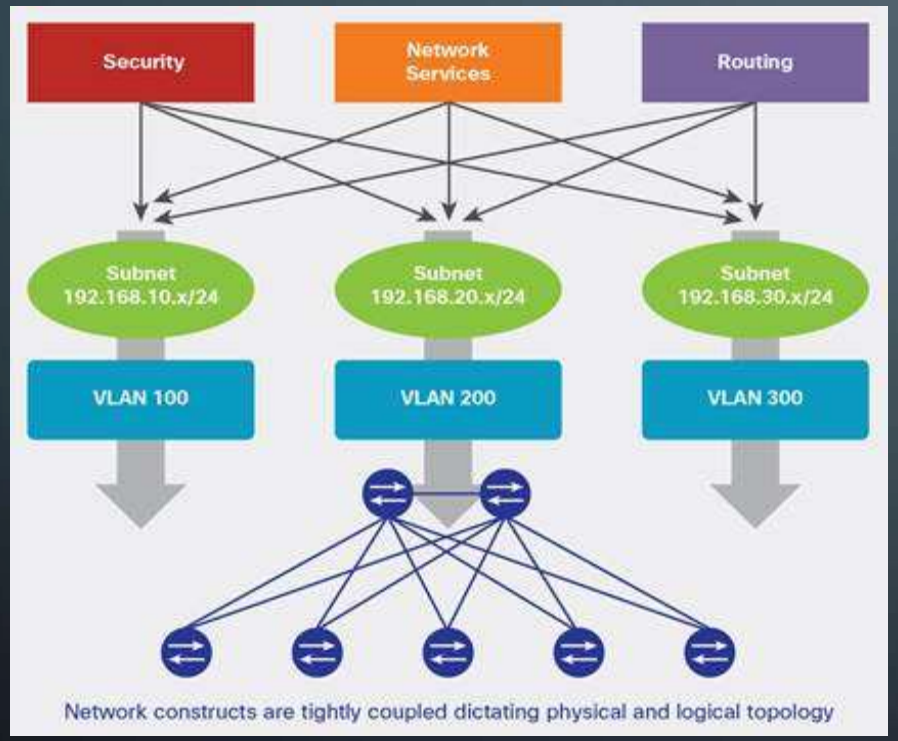


Aplicação: Ecossistema completo que fornecem o resultado final ao utilizador

ANTIGAS ESTRUTURAS DE REDE PARA APLICAÇÕES

- Pedras Basilares:
  - VLAN's
  - SUBREDES
- Objectivo:
  - Segmentação para gestão/segregação de tráfego
  - Implementação de políticas de roteamente e segurança

ANTIGAS ESTRUTURAS DE REDE PARA APLICAÇÕES



1. Aplicações agrupadas por VLAN's e por subredes
2. Conectividade baseada em roteamento
3. Serviços associados aos endereços da subrede

Problemas:

- Restrições à forma de agrupar aplicações
- Tendência para configurações incorretas
- Configuração de políticas demasiado latas
- Lentidão na implementação
- Reduzida auditoria

Modelo antigo de mapeamento entre as Aplicações e a Rede cria um impacto negativo significativo no negócio

É necessário um novo modelo de mapeamento entre as Aplicações e a Rede de modo a potenciar o negócio

Endpoint Groups

EPG

ENDPOINT GROUPS

- Endpoint Groups (EPGs) fornecem um novo modelo de mapeamento entre as Aplicações e a Rede
  - Não utilizam endereçamento ou VLAN's para implementação de conectividade e políticas de segurança
  - São contentores de grupos de aplicações ou componentes de aplicações, sobre os quais podem ser aplicadas lógicas de reencaminhamento e de políticas de segurança
  - Permitem a separação do reencaminhamento e da política de segurança do endereçamento

ENDPOINT GROUPS

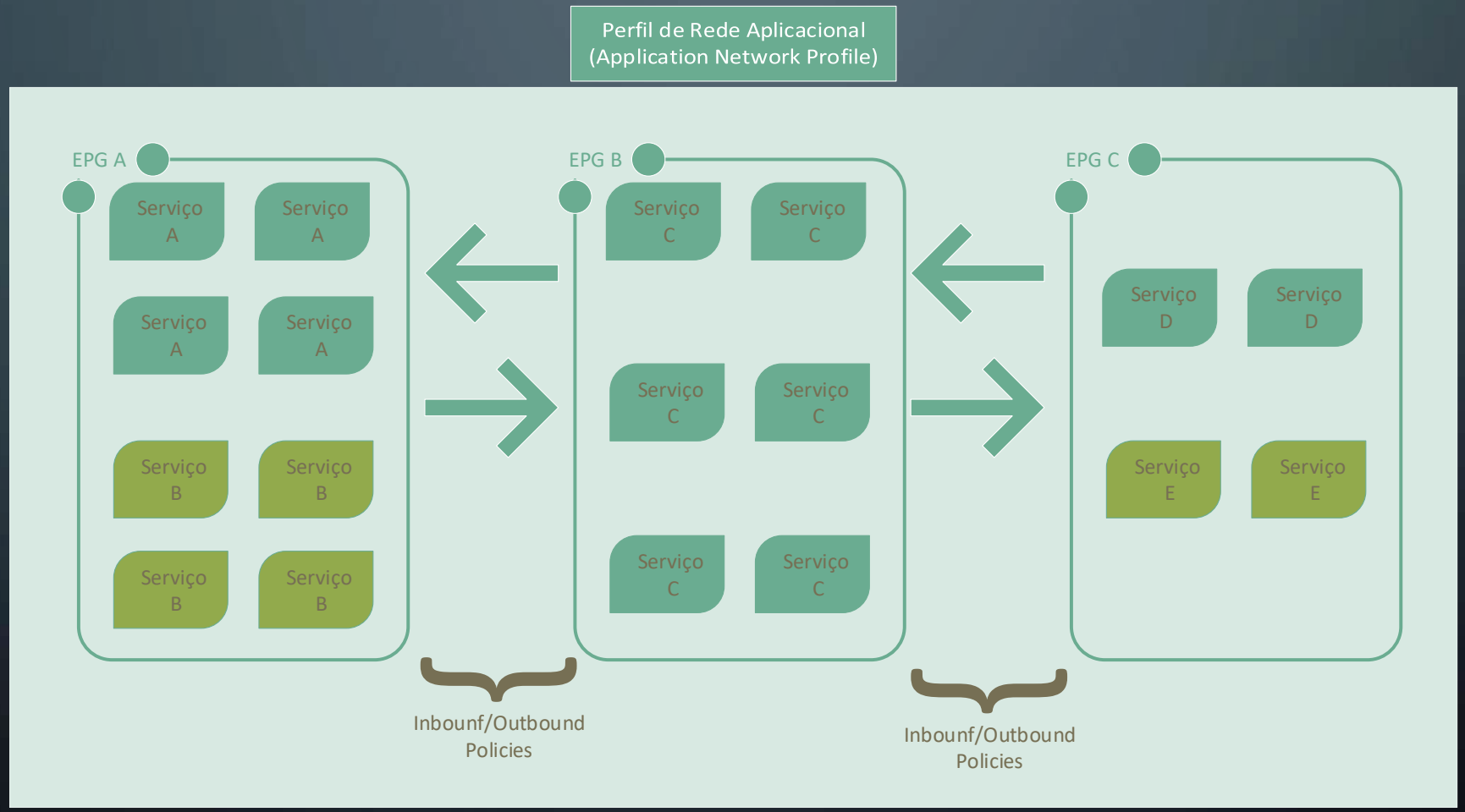
ENDPOINT GROUPS

- Mapeamento:
  - Aplicações com a Rede
  - Donos e *developers* de Aplicações com a Rede
  - Estágio de maturidade das Aplicações (desenvolvimento, teste, produção) com a Rede
  - Funcionalidades das Aplicações com a Rede

APPLICATION NETWORK PROFILE

- Nível conceptual superior da estrutura da Rede
  - Agrupamento de um ou mais EPG's
  - Políticas de comunicação entre os EPG's (Contratos)
  - Definição de conectividade entre níveis aplicacionais
    - Web-app-database
    - Compute-network-storage
- Instâncias de uma aplicação/Sistema de informação completo na rede

APPLICATION NETWORK PROFILE



EPG'S & APPLICATION NETWORK PROFILE

- EPG's
  - Agrupam components comuns de uma aplicação completa
  - São agrupados com as comunicações e políticas entre EP
- Application Network Profile (ANP)
  - Agrupam os EPG's e os respectivos contratos que definem as políticas de interconectividade entre eles.

COMO ATINGIR OS OBJECTIVOS?

VMware

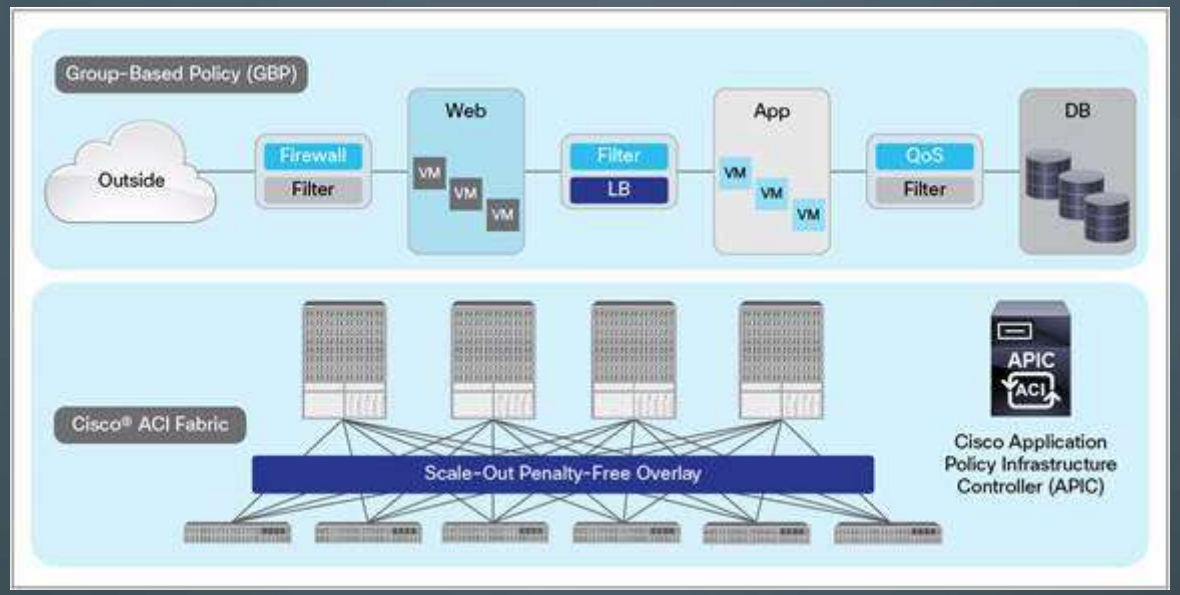
NSX

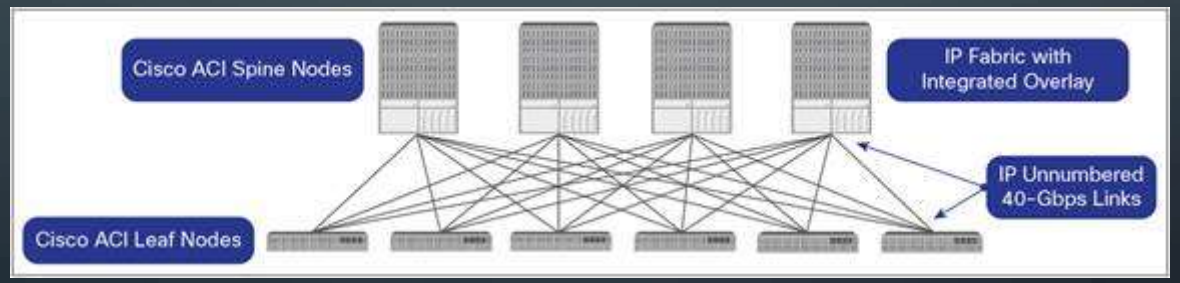
COMO ATINGIR OS OBJECTIVOS?

Cisco

Application Centric Infrastructure

ACI





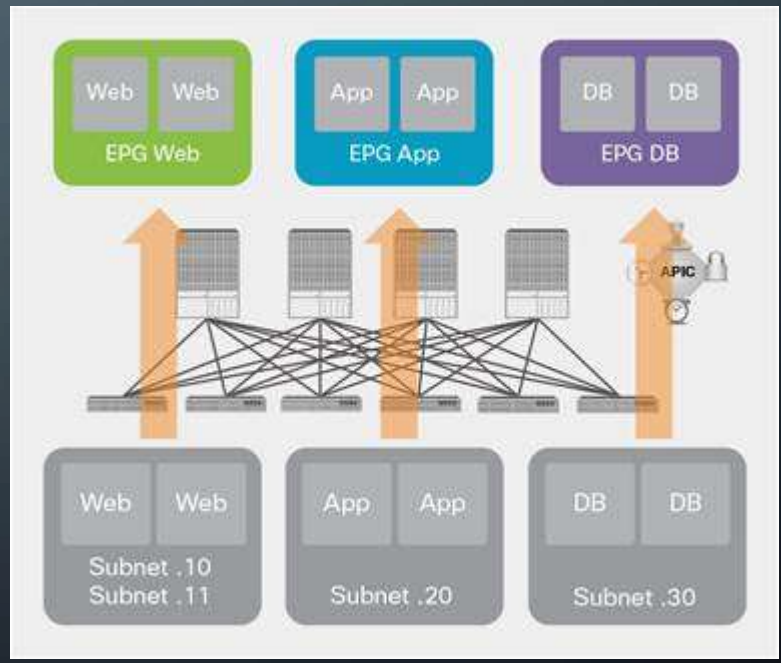
De facto a tecnologia está presentemente nos 100Gb/s

ENTRELAÇADO ACI (ACI *FABRIC*)

- O entrelaçado ACI permite facilmente
  - Instanciação de políticas
  - Inserção de serviços
- Diferentes visões do todo
  - Grupos de componentes aplicacionais
  - Maturidade aplicacional
  - Zonas

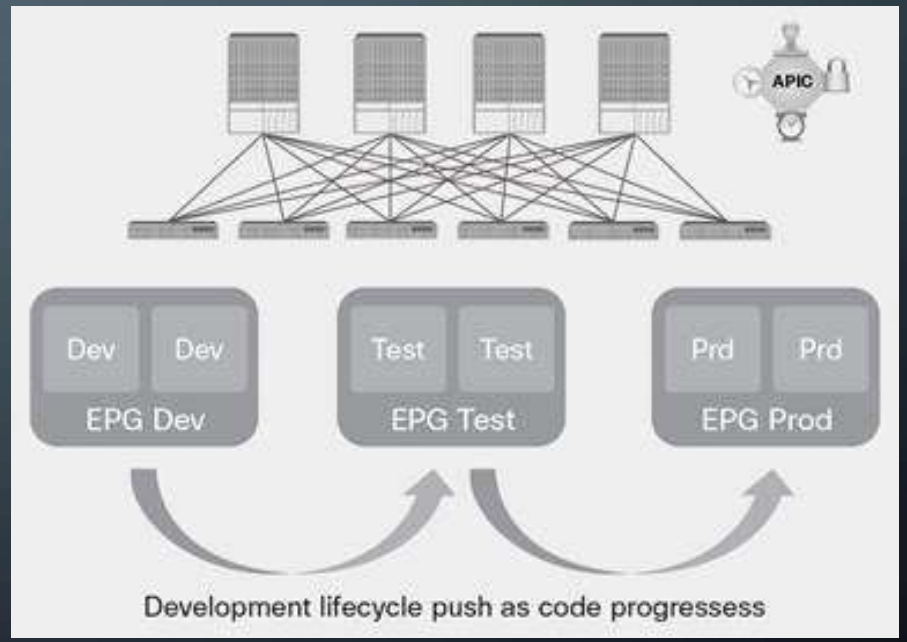
ENTRELAÇADO ACI

- EPG como grupo de componentes aplicacionais
  - Servidores web
  - Servidores de webservices
  - Servidores aplicacionais
  - Servidores de Bases de Dados
  - etc



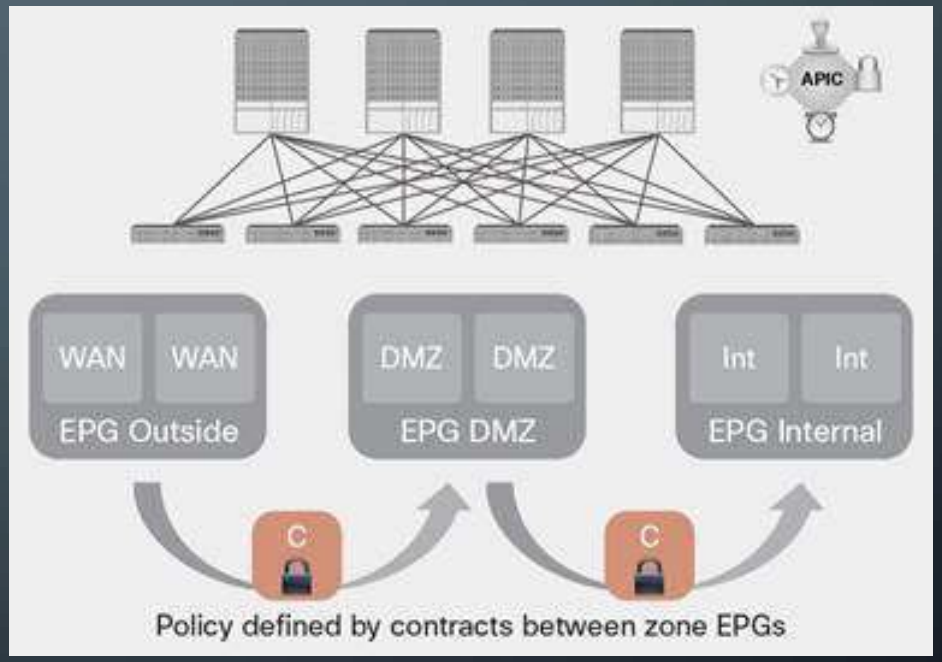
ENTRELAÇADO ACI

- EPG como fase de maturidade da aplicação
  - Desenvolvimento
  - Teste
  - Produção
  - Desmantelamento (*decommissioning*)



ENTRELAÇADO ACI

- EPG como zona
  - Externa
  - DMZ
  - Interna
  - Interna (PCI)
  - etc



GESTÃO DO ENTRELAÇADO ACI

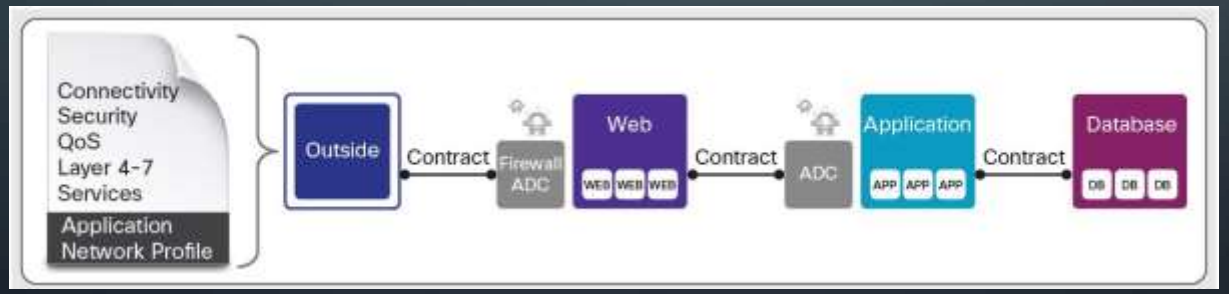
- APIC – Cisco Application Policy Infrastructure Controller
  - Tenant (Customer, BU, Group)
  - Private Network (Context, VRF)
  - Bridge Domain (L2 Boundary)
  - IP Spaces (Subnets)
  - EPG
  - Contract

SEGURANÇA DO ENTRELAÇADO ACI

- Modelo de política centrada na Aplicação
  - Abordagem anterior baseada em:
    - Topologia de rede estática
    - Actualização manual dos equipamentos, particularmente dos equipamentos de segurança (firewall, IDS, IPS)
  - Desacoplamento entre política e topologia da rede
  - Equadramento aberto das políticas, expressas em termos aplicacionais

SEGURANÇA DO ENTRELAÇADO ACI

- Políticas definidas em termos de linguagem aplicacional
  - Endpoint Group (EPG)
  - Contrat
  - Aplication Network Profile (ANP)



SEGURANÇA DO ENTRELAÇADO ACI

- Modelo de segurança baseado em *whitelisting*
  - Suporte para o modelo de confiança Zero
  - Não há confiança entre entidades independentemente da sua localização
- Para que haja conectividade entre EPG's é necessário um contrato explícito
  - Permissão
  - Negação
  - Log
  - Reencaminhamento
  - etc.

SEGURANÇA DO ENTRELAÇADO ACI

- Contratos entre EPG's são independents da localização física dos EPG's
- Alteração da localização física de EPG's na rede implicam "arrastamento" dos contratos
- Automatização e Gestão centralizada via APIC
  - GUI
  - JSON
  - REST API

SEGURANÇA DO ENTRELAÇADO ACI

- Moldura aberta e extensível a terceiros (OpFlex)
  - A10 networks
  - Citrix
  - Embrane
  - F5
  - Radware

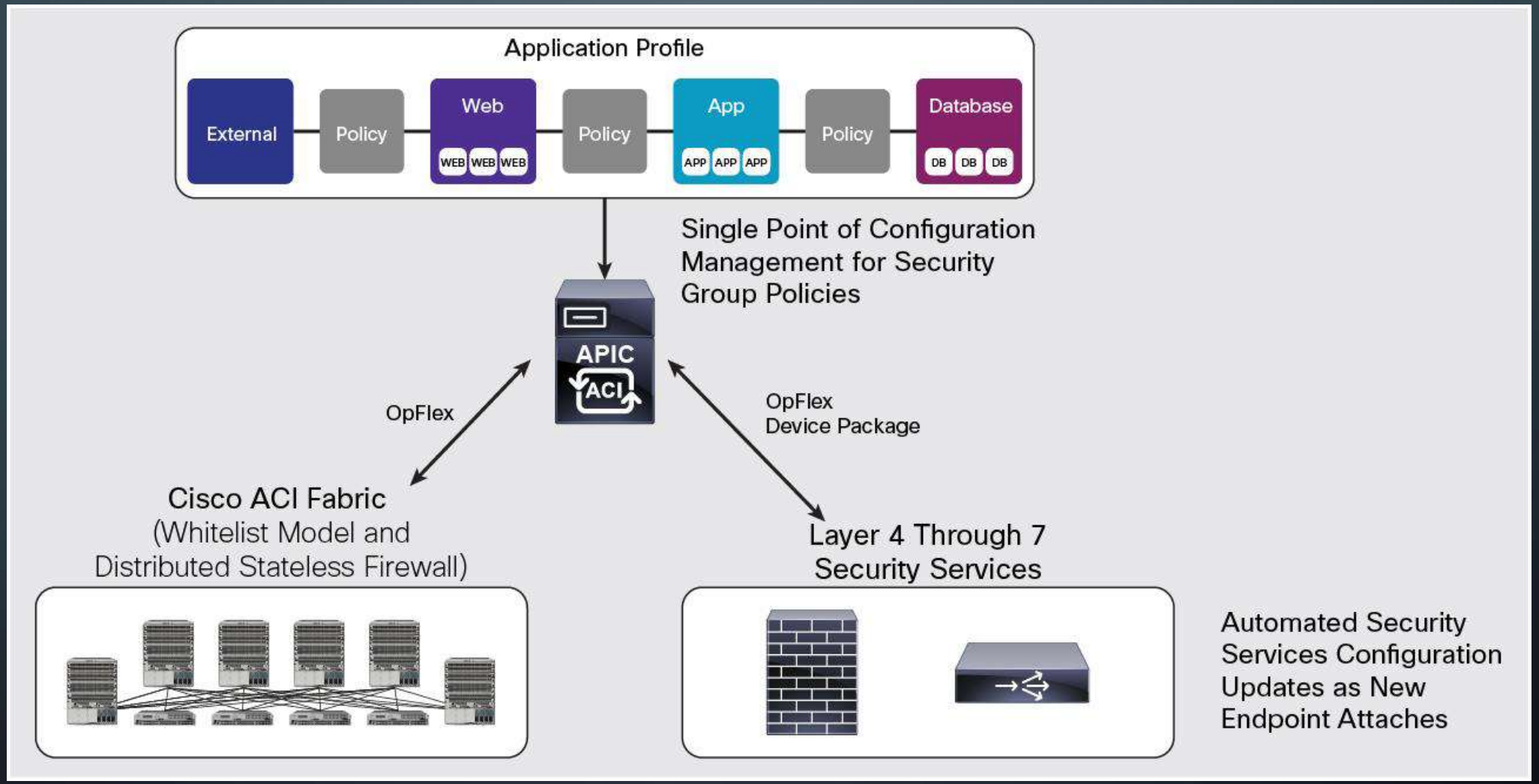
SEGURANÇA DO ENTRELAÇADO ACI STATELESS FIREWALL

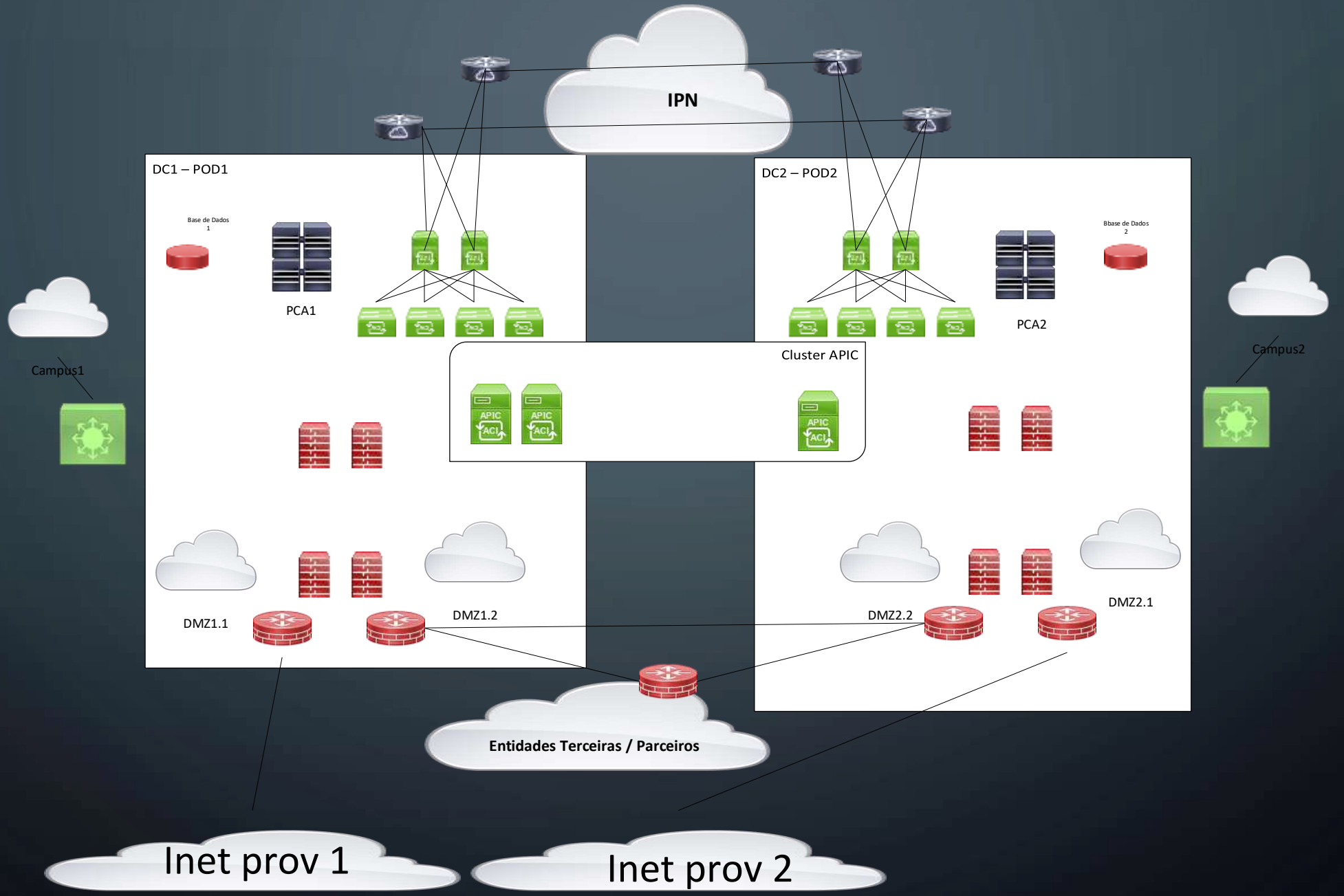
Contrato entre EPG's

Microsegmentação

IMPLEMENTAÇÃO DA SEGURAÇA NO ACI STATEFULL FIREWALL

- Bare Metal
  - ASA 5585-X
- Virtualização
  - ASAv – Adaptive Security Virtual Appliance
- Objectivo: Completa Integração no ACI


Application Profile
External
Policy
Web
WEB WEB WEB
Policy
App
APP APP APP
Policy
Database
DB DB DB
Single Point of Configuration Management for Security Group Policies
APIC
ACI
OpFlex
OpFlex Device Package
Cisco ACI Fabric
(Whitelist Model and Distributed Stateless Firewall)
Layer 4 Through 7 Security Services
Automated Security Services Configuration Updates as New Endpoint Attaches


IPN
DC1 – POD1
Base de Dados 1
PCA1
DC2 – POD2
Bbase de Dados 2
PCA2
Cluster APIC
APIC
ACI
Campus1
Campus2
DMZ1.1
DMZ1.2
DMZ2.2
DMZ2.1
Entidades Terceiras / Parceiros
Inet prov 1
Inet prov 2

Q&A

ATENÇÃO! ATENÇÃO!
¡¡¡¡¡¡¡¡¡ FALHA CRÍTICA NA ORGANIZAÇÃO !!!!!!!!!

Temos os ovos todos no mesmo cesto!

FIM DO FIM

Mui grato pela vossa atenção

Paulo Machado pjcmachado@gmail.com +258 823500060