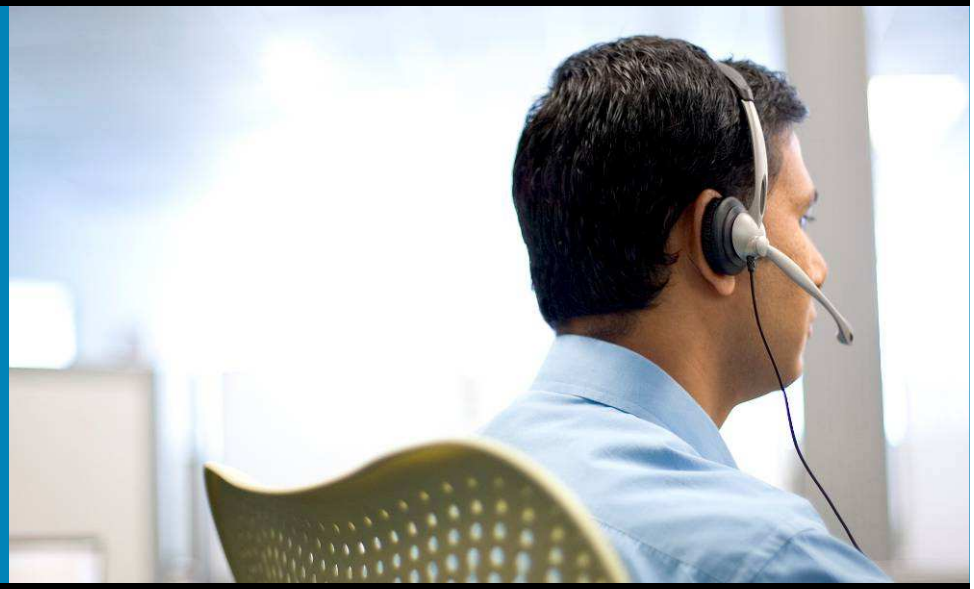
Melhores Práticas para Segurança de Redes

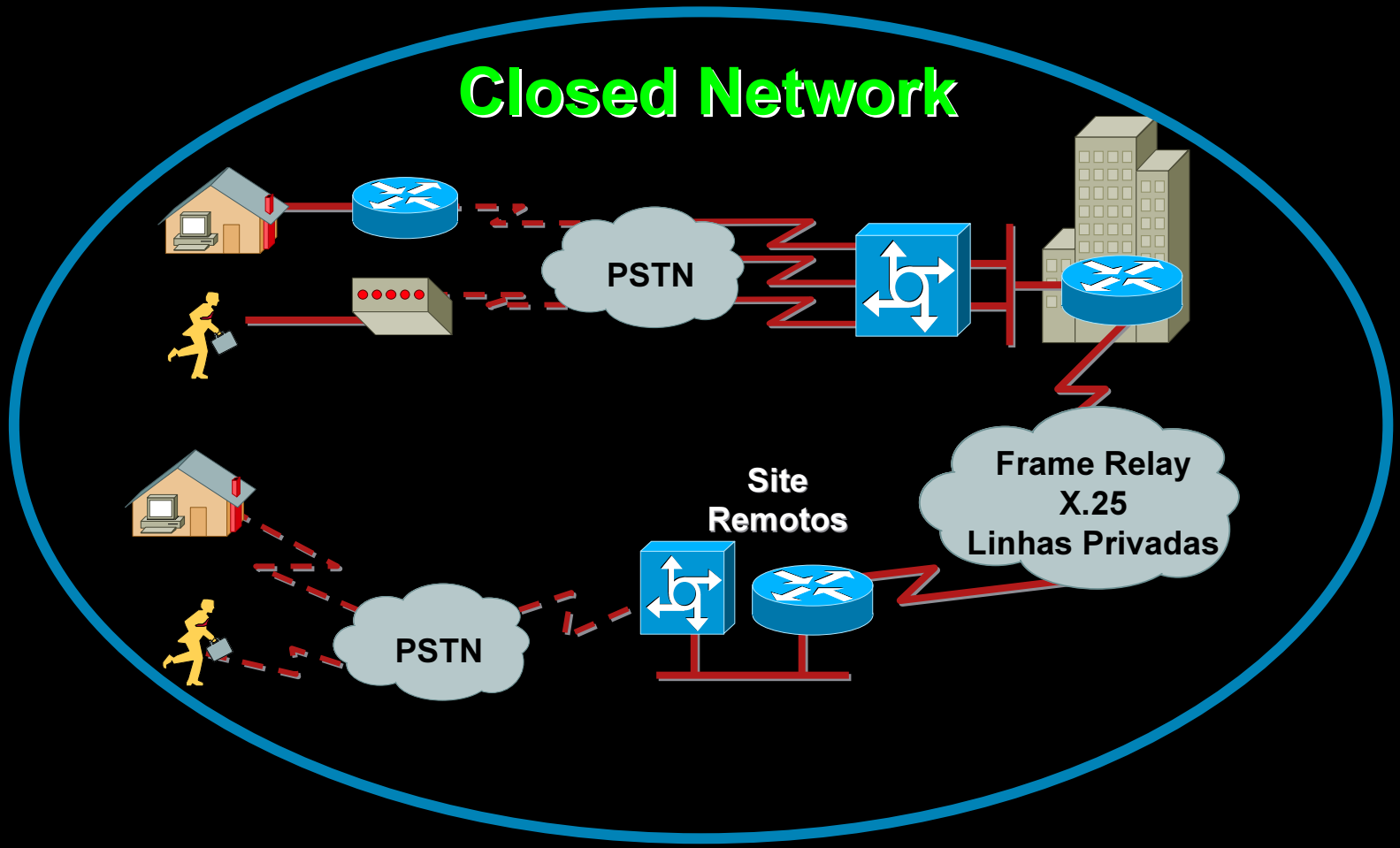


Andrey Lee
Engenheiro de Sistemas
Service Providers

GTS - 09
30 / Maio / 2007

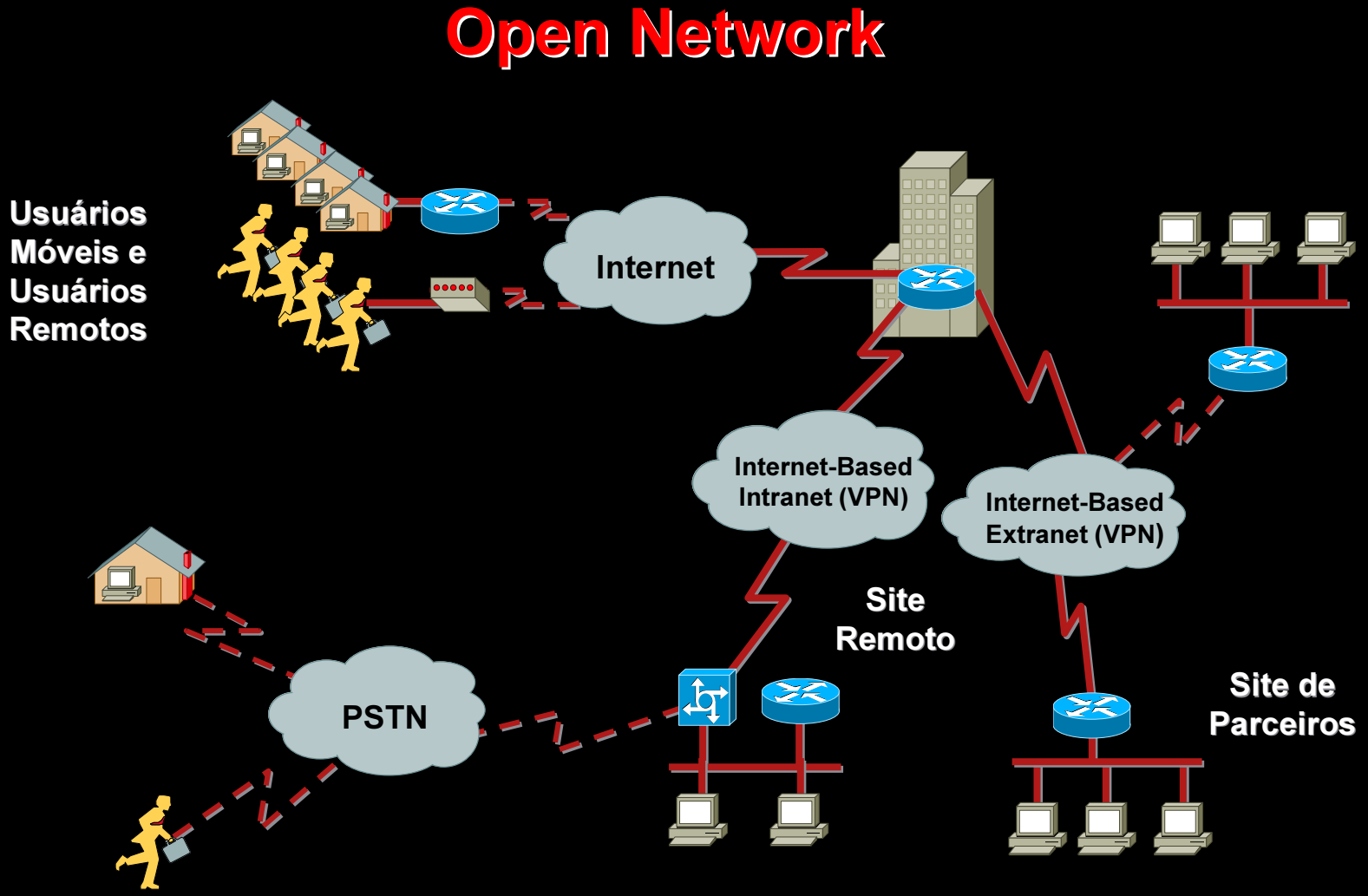
© 2007 Cisco Systems, Inc. All rights reserved.

Redes Corporativas – Cinco anos atrás



© 2007 Cisco Systems, Inc. All rights reserved.

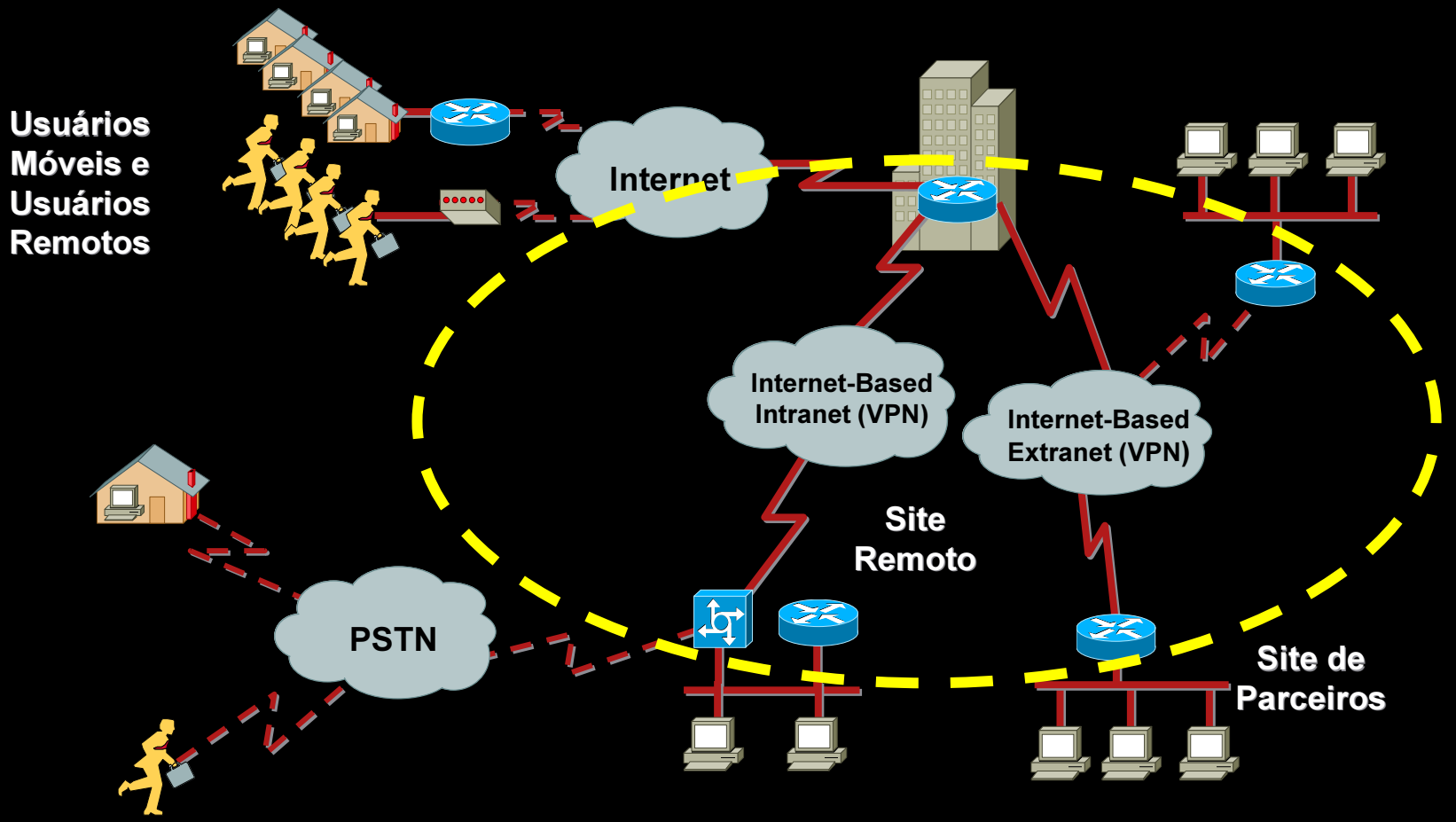
Redes Corporativas - Hoje



© 2007 Cisco Systems, Inc. All rights reserved.

Redes Corporativas – Onde queremos chegar ?

Flexibilidade versus Segurança



© 2007 Cisco Systems, Inc. All rights reserved.

Entendendo as Ameaças

- Internas
  - Erro Humano (ex.: fat finger attack)
  - Funcionário Malicioso
- Externas
  - Worms
  - Packet floods
  - Bugs
  - Intrusão
  - Ataques de Serviço (DNS, voice, etc.)

© 2007 Cisco Systems, Inc. All rights reserved.

Configuração de Roteadores: Métodos Tradicionais

- Desabilite protocolos não usados

```
no service tcp-small-servers
no cdp run
```

- ACLs de terminal virtual (Telnet)
- ACL de SNMP
- Desabilite SNMP RW
  - Use SNMPv3 para RW se necessário
- Cuidado com sessões de TCP inativas

```
service tcp-keepalives-in
```

- Aplique QoS na borda da rede
- Habilite todas as senhas do roteador, inclusive encriptação
- Use AAA, SSH
- Habilite SYSLOG e NTP
- Desabilite funcionalidades desnecessárias

```
no ip directed-broadcast
no ip proxy-arp
no ip redirects
```

© 2007 Cisco Systems, Inc. All rights reserved.

Configuração de Roteadores: Métodos Tradicionais

- Valide o endereço de origem (RFC2827 / BCP38, RFC3704 / BCP84)

```
ip verify unicast source reachable-via {any|rx}
cable source-verify [dhcp]
ip verify source [port-security]
```

- Desabilite source-routing

```
no ip source-route
```

- Aplique Listas de Prefixo em peers eBGP
- Habilite BGP dampening nas interfaces BGP
- Autenticação MD5 em BGP e IGP

- Funcionalidades baseadas em Hardware
  - –Controle a geração de mensagens ICMP unreachable (destino não alcançável)

```
ip icmp rate-limit unreachable
ip icmp rate-limit unreachable DF
interface null0
 no ip unreachables
```

  - –Garanta CPU para gerenciamento

```
scheduler allocate
```

  - –Selective Packet Discard (SPD)

© 2007 Cisco Systems, Inc. All rights reserved.

Configuração de Rede: ACLs de Infraestrutura

- Premissa Básica: filtrar tráfego destinado para seus roteadores de core
  - Será que seus roteadores realmente precisam processar todos os tipos de lixo ?
- Desenvolva uma lista de protocolos necessários que são originados de fora de seu AS e acessam seus roteadores de core
  - Exemplo: eBGP peering, GRE, IPSec, etc.
  - Use classificação em ACL se necessário
- Identifique seus blocos de endereço de core
  - Este é o espaço de endereços protegidos
  - Sumarização é críitica → ACLs simples e pequenas

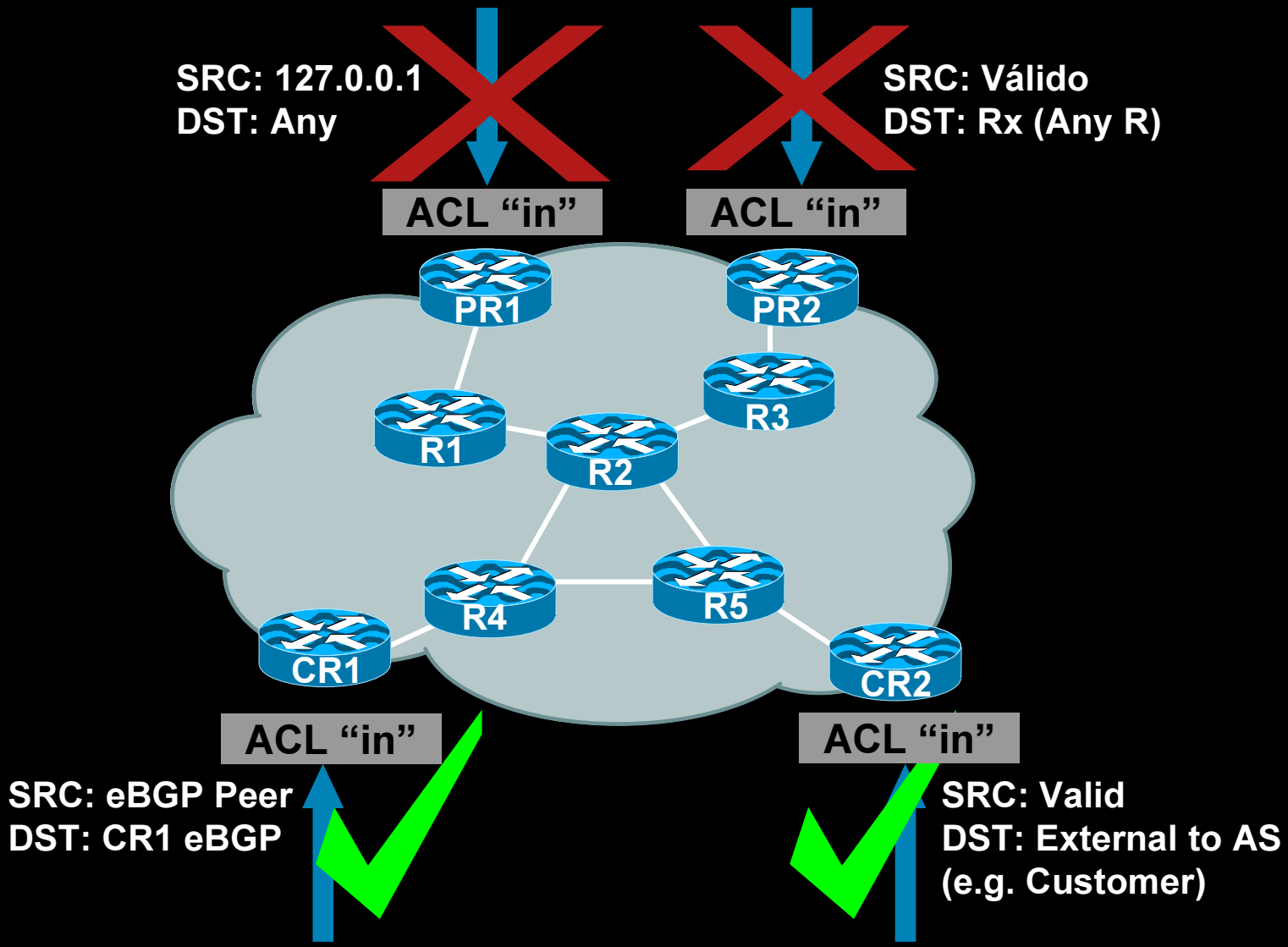
© 2007 Cisco Systems, Inc. All rights reserved.

Configuração de Rede: ACLs de Infraestrutura

- Infrastructure ACL permitirá somente os protocolos necessário e bloqueará todos os outros
- ACL dele prover também filtragems ‘anti-spoofing’
  - Bloqueie seu espaço de fontes externas
  - Bloqueie o espaço da RFC1918
  - Bloqueie endereços de multicast (224/4)
  - RFC3330 define o uso especial de IPv4

© 2007 Cisco Systems, Inc. All rights reserved.

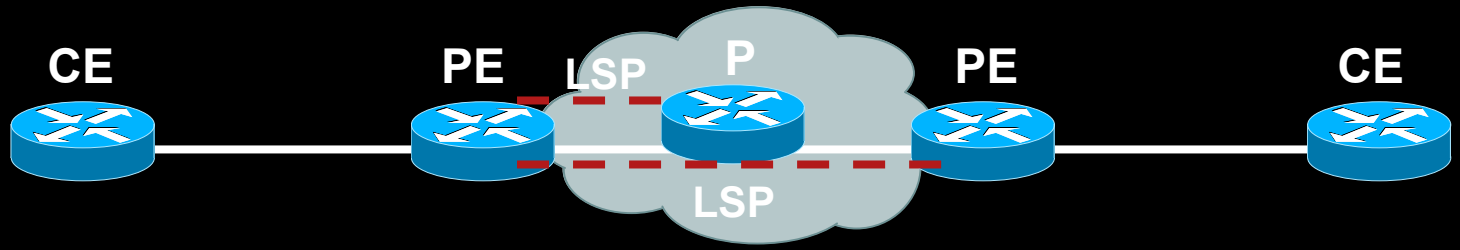
Configuração de Rede: ACL de Infraestrutura em ação



© 2007 Cisco Systems, Inc. All rights reserved.

Configuração de Rede: RFC2547 (MPLS) VPN

- Coloque todos seus clientes, inclusive a Internet, dentro de VRFs distintas em uma rede IP/MPLS
- O core se tornará invisível e inalcançável
- Somente a prórpia rede e o NOC devem existir na tabela de roteamento global



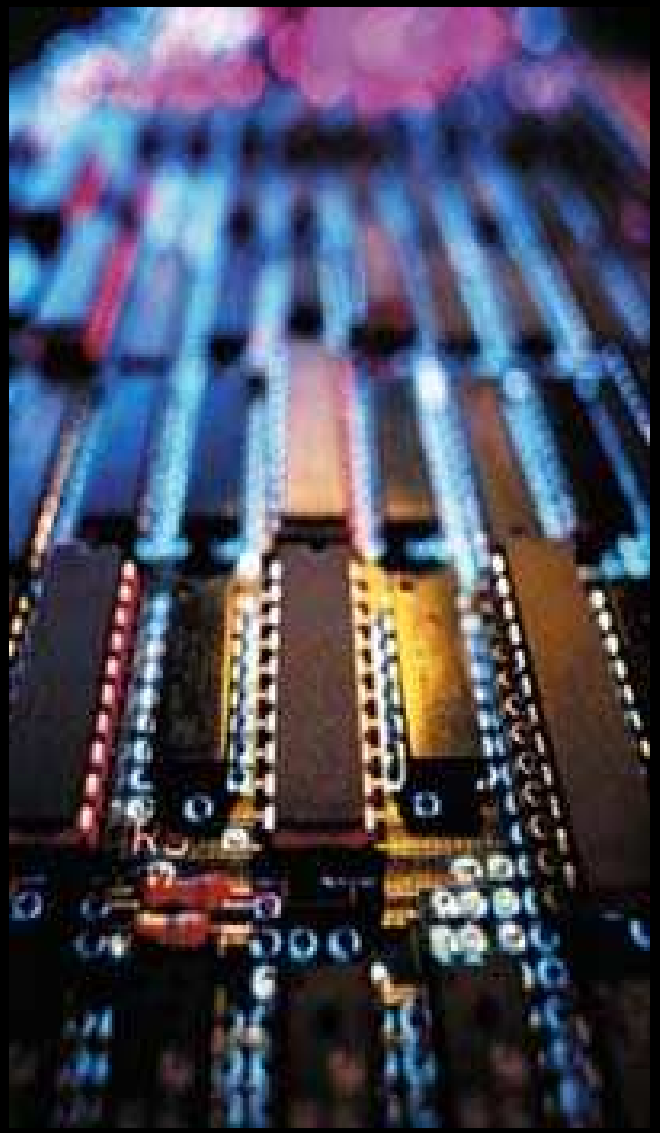
- Mecanismos de segurança adicionais devem ser implementados nos PEs

© 2007 Cisco Systems, Inc. All rights reserved.

Resumindo…

- As ameaças vieram para ficar, estão mudando, e precisamos evoluir
- Nosso mundo conectado é o alvo, não um pedaço ou uma empresa
- *Estratégia de Segurança Integrada* é como devemos encarar estes desafios …

Conhecimento de segurança será tão importante quanto conhecimento de IP



© 2007 Cisco Systems, Inc. All rights reserved.

Links Interessantes…

- iACL Deployment Guide
  - http://www.cisco.com/warp/public/707/iacl.html
- rACL Deployment Guide
  - http://www.cisco.com/warp/public/707/racl.html
- CoPP Deployment Guide
  - http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_white_paper09186a0080211f39.shtml
- Cisco Network Foundation Protection (NFP)
  - http://www.cisco.com/warp/public/732/Tech/security/infrastructure/
- SP Security Archive
  - ftp://ftp-eng.cisco.com/cons/isp/security/
- NANOG
  - http://www.nanog.org/previous.html
  - http://www.nanog.org/ispsecurity.html

© 2007 Cisco Systems, Inc. All rights reserved.

Outros documentos de Melhores Práticas

- Muitas organizações publicam guias de melhores práticas sobre segurança em roteadores
- Além dessa apresentação, indicamos:

  http://www.first.org/resources/guides/

  http://www.sans.org/resources/policies/

  http://www.ietf.org/html.charters/opsec-charter.html
- Esses sites possuem uma documentação bem completa em termos de ‘Melhores Práticas’, especialmente no que se refere a métodos tradicionais de configuração de roteadores.

© 2007 Cisco Systems, Inc. All rights reserved.

OBRIGADO !!!

© 2007 Cisco Systems, Inc. All rights reserved.

PERGUNTAS ???

© 2007 Cisco Systems, Inc. All rights reserved.