Protegendo seu zSeries na Internet

Vicente Ranieri Junior

Certified I/T Specialist Consultant

Latin America zSeries Technical Support Team

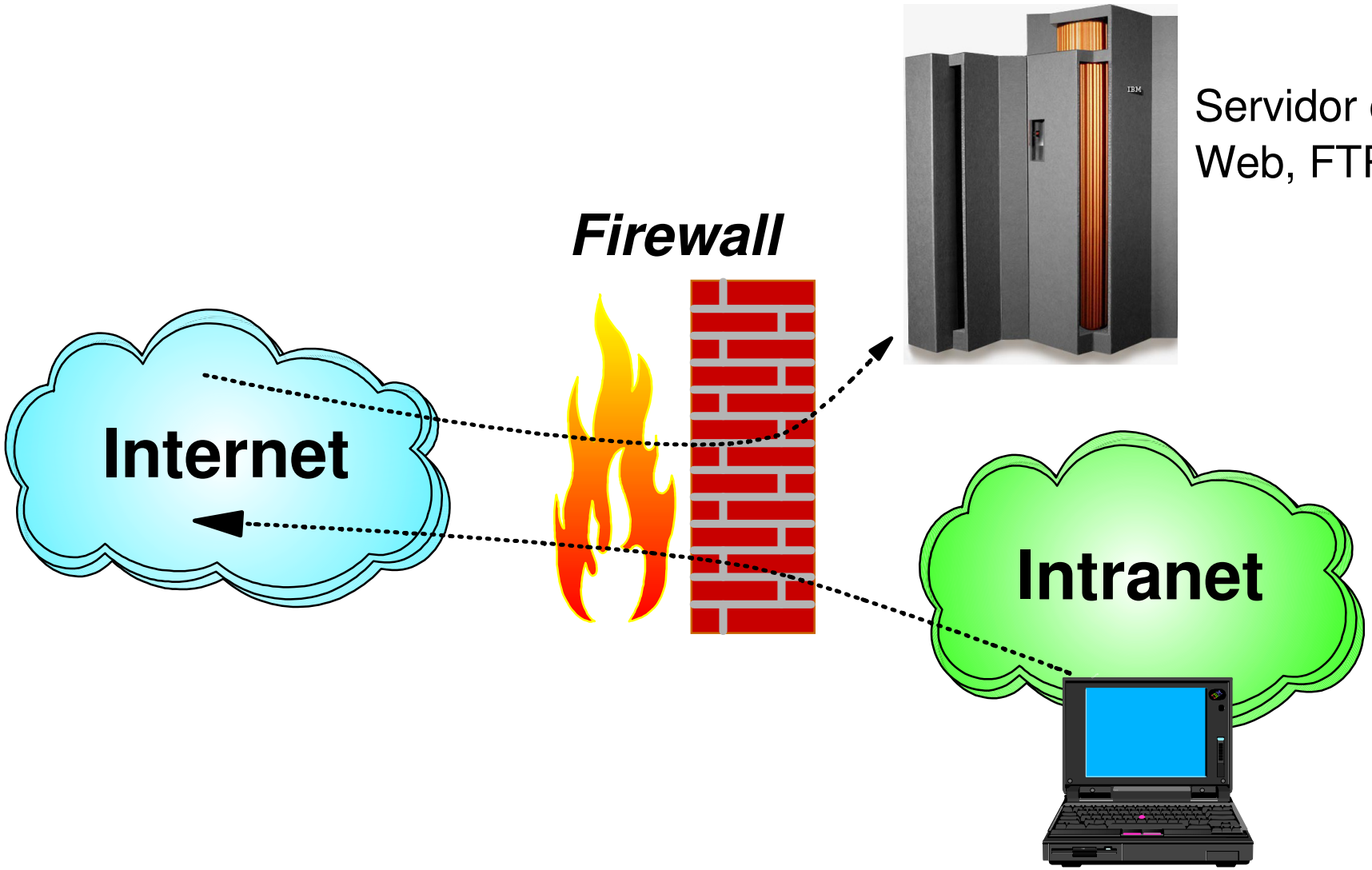
ranieri@br.ibm.com

Agenda

- **Firewalls**
- **Zonas Desmilitarizadas (DMZ)**
- **Protegendo o TCP/IP com RACF**
- **Serviços de Detecção de Intrusão (IDS)**
- **Protegendo o *Unix System Services* com RACF**
- **Cenário com zSeries na Internet**

FIREWALLS

Conceito de *Firewall*



Filtros de Pacote IP

- **Filtro de Pacote IP Básico**
  - **Inspeciona campos nos *headers* IP e TCP**
  - **Permite o acesso ou descarta pacotes baseado no endereço IP, número da porta,tipo de pacote (TCP SYN,TCP ACK),direção,etc.**
  - **Vantagem: Simples, baixo custo de operação**
  - **Desvantagem: estático, não detecta certos tipos de ataques**
- **Inspeção de Pacote IP**
  - **Mantém a informação baseado na origem e no destino**
  - **Pode permitir o acesso a certas portas baseado em negociações anteriores**
  - **Vantagem: Pode limitar o tráfego vindo de uma única origem, podendo detectar certos tipos de ataque**
  - **Desvantagem: Requer um consumo maior de CPU e memória, propenso a novos tipos de ataques, maior complexidade**

Servidores *Proxy* (Procurador)

- **O cliente se conecta a um servidor *proxy*, que irá representar o cliente perante o servidor real**
- **Requer um servidor *proxy* diferente para cada protocolo**
  - ***Proxy* para FTP, *proxy* para telnet, *proxy* para HTTP,...**
- **Vantagens**
  - **O servidor *proxy* conhece o protocolo, podendo inspecionar comandos e dados**
  - **Autenticação de clientes em um servidor *proxy* é uma opção**
  - **Alguns servidores *proxy* podem armazenar (*cache*) dados acessados por diversos clientes**
- **Desvantagens**
  - **Alto consumo de CPU e memória**
  - **Clientes devem conhecer e configurar o endereço do *proxy***

Servidores *SOCKS*

- **O cliente se conecta a um servidor *SOCKS*, o qual retransmite o pacote para o servidor real baseado em opções de configuração**
- **Um servidor *SOCKS* atende a todos os protocolos TCP**
- **Autenticação de cliente é uma opção com *SOCKS V5***
- **Vantagens: consumo de CPU e memória menor que o de servidores *proxy***
- **Desvantagens:**
  - **Retransmite pacotes, não inspeciona o conteúdo dos pacotes**
  - **O endereço do servidor SOCKS deve ser conhecido e configurado pelos clientes**
  - **Os clientes devem suportar *SOCKS* (devem ser *socksified*)**

z/OS Firewall Technologies

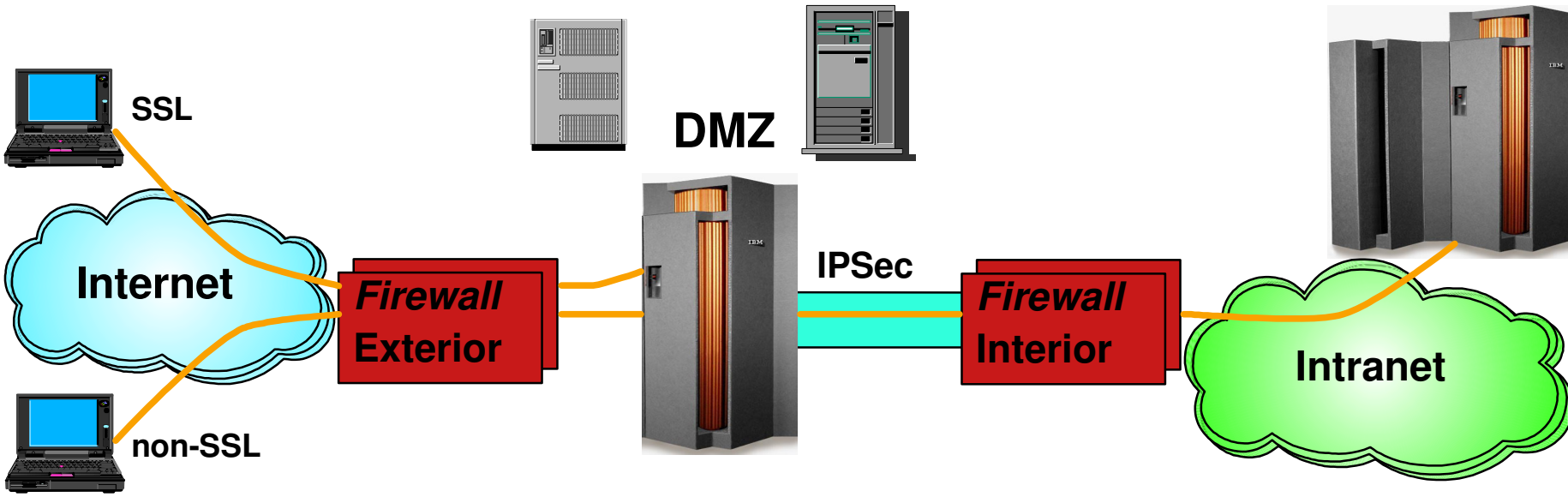
- **Principais funções:**
  - **Filtro de pacote IP básico**
  - **IPSec *Virtual Private Networking* (VPN) com suporte a IKE**
  - **GUI de configuração baseada em Java**
    - **Administração com conexão cliente-servidor suportando SSL**
- **Recomendações:**
  - **Utilize o filtro de pacote IP básico para proteger um sistema OS/390 ou z/OS das redes conectadas a ele.**
    - **É uma função de baixo custo que pode prover segurança adicional contra problemas inexperados na rede ou contra brechas no *firewall* externo**
  - **Não utilize como *firewall* de roteamento**
    - **Carente de funções nesta área**
    - **Nenhum desenvolvimento esta previsto para funções de *firewall* de roteamento**

Zonas Desmilitarizadas (DMZ)

Zonas Desmilitarizadas (DMZ)

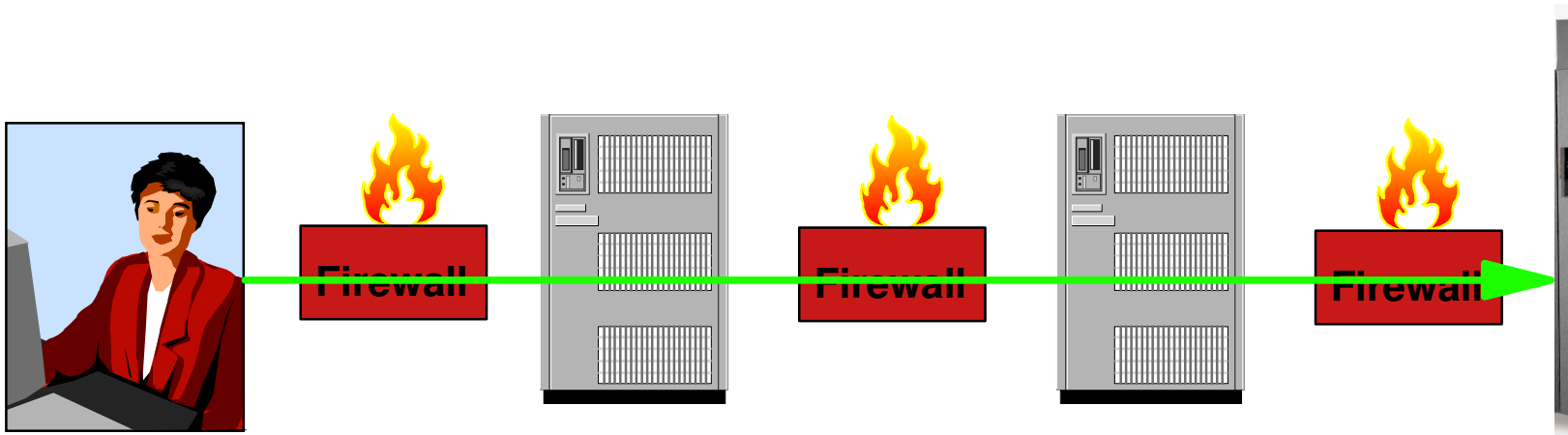
- **Geralmente vista como uma rede entre a Internet e a Intranet**
  - **É comum *firewalls* separarem a DMZ da Internet e da Intranet**
- **Contém servidores que necessitam ser acessados pela Internet**
  - **Servidores HTTP, servidores FTP, servidores DNS**
- **Servidores na DMZ necessitam acessar os sistemas corporativos**
  - **Do contrário, não haveria necessidade de conectar a DMZ a Intranet**
- **Existem várias configurações de DMZ com complexidade variável**
  - **O nível de confiança nos servidores na DMZ influenciarão o desenho desta DMZ**

DMZ - Desenho Básico



- **O *firewall* exterior permite o tráfego apenas até os servidores na DMZ**
  - O tráfego pode ser SSL ou non-SSL dependendo da criticidade dos dados
- **Dados podem ser trocados entre os servidores na DMZ e os servidores corporativos na Intranet através do *firewall* interior**
  - O *firewall* interior permite somente tráfego da DMZ
  - O tráfego pode ser protegido por protocolos de segurança quando necessário
  - IPSec pode ser utilizado para autenticar-se ao *firewall* interior ou ao sistema na Intranet

Mundo UNIX e Windows



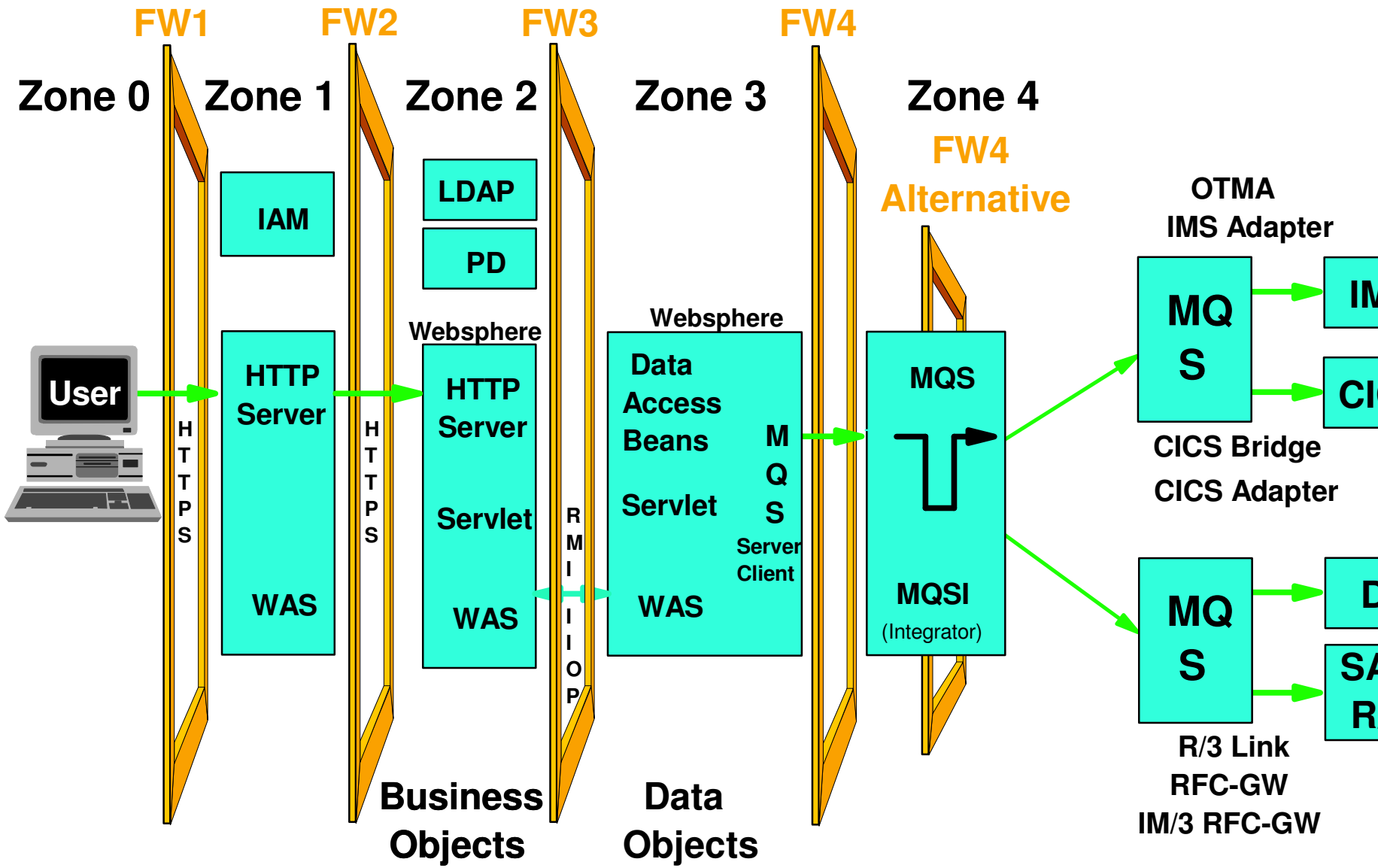
WEB Servers

Application Servers

Alguns comentários sobre este *design*

- **Em muitos casos, marcas diferentes de firewalls são utilizadas**
  - **Se um *firewall* falhar, o próximo irá (pelo menos esperamos que) bloquear o ataque**
- **Em geral uma mudança de protocolos (HTTP, RMI/IIOP, ITOC) ocorre em cada *firewall***
  - **Se um intruso encontra uma maneira de comprometer um protocolo, isto deve ser parado no próximo *firewall***
- **Em sistemas onde *buffer overflows* e outras vulnerabilidades permitem a um intruso ganhar um usuário *root* ou administrador, o efeito de toda esta proteção é questionável.**

O zSeries necessita deste *design* ?

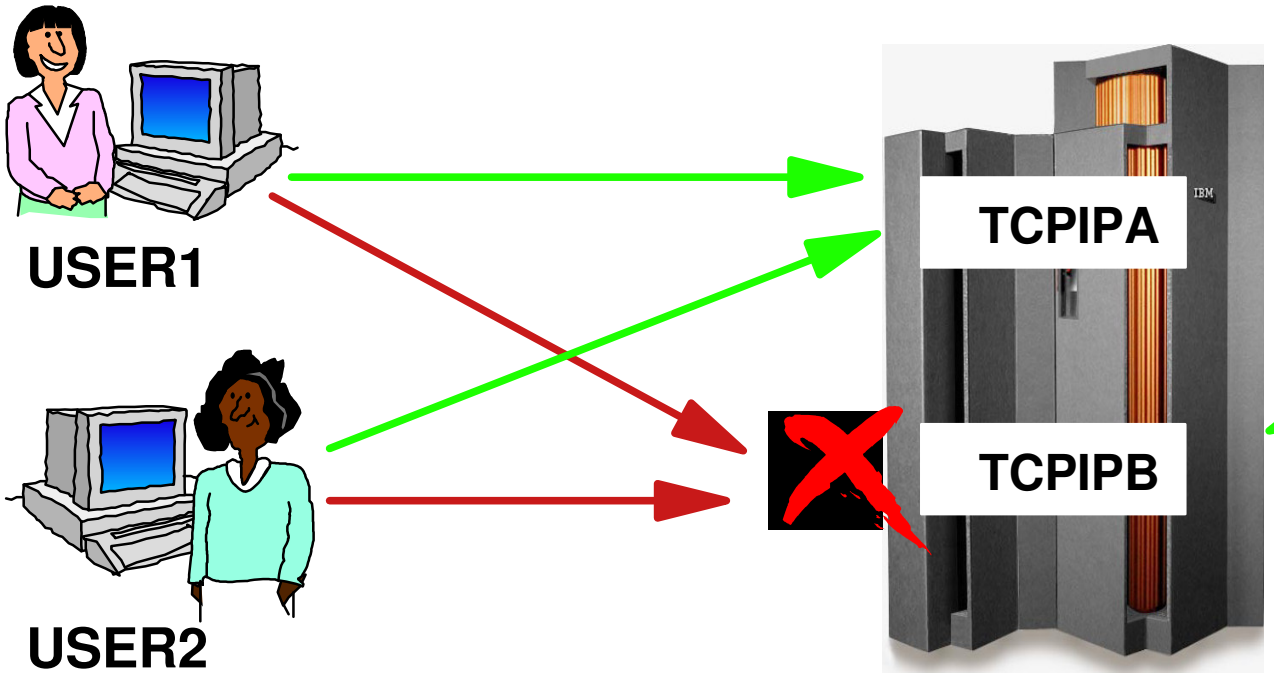


Protegendo TCP/IP com RACF (OS/390 V2R10)

Protegendo Pilhas, Portas e Acesso a Rede com RACF

- **Novo conceito de proteção para o TCP/IP**
  - **Baseado na autenticação de usuários RACF no OS/390**
  - **Pode prevenir o acesso não autorizado a Internet**
  - **Pode prevenir ataques internos do tipo Cavalo de Tróia**
- ***Firewall* controla endereços IP e portas**
  - **Não pode prevenir o uso de pilhas e portas por usuários não autorizados**
  - **Não pode permitir facilmente o acesso a rede pelos servidores enquanto restringe outros usuários**

Controle de Acesso a Pilha TCP/IP



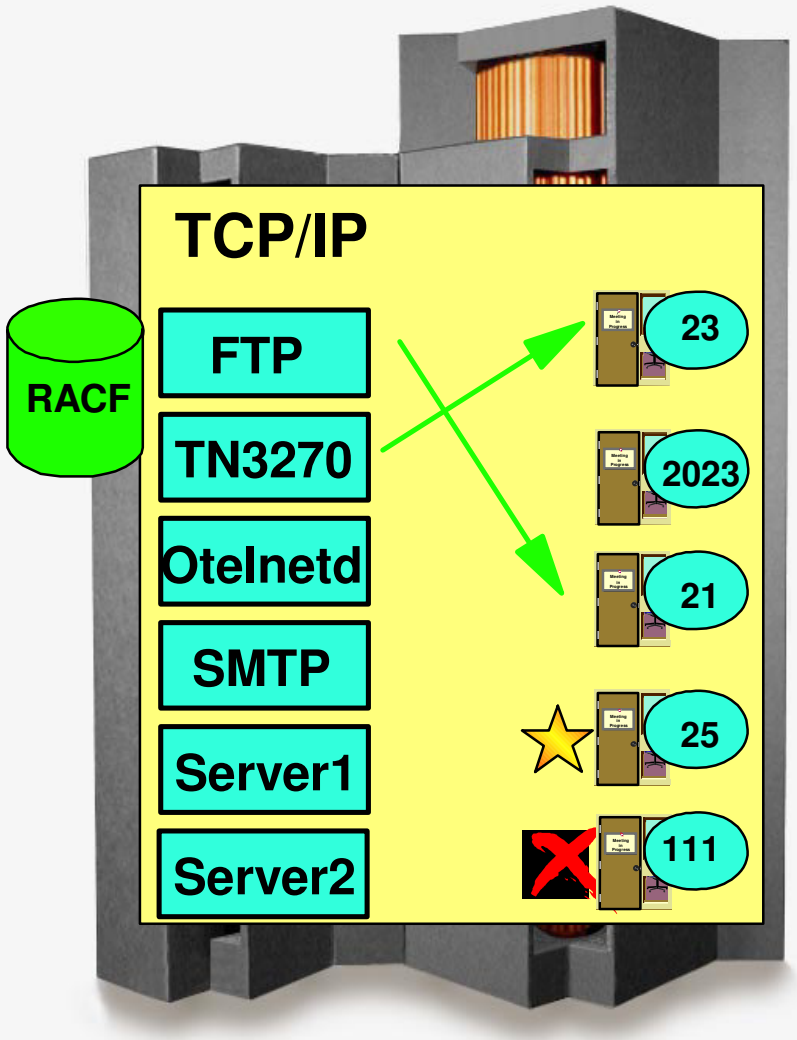

```
SETROPTS CLASSACT(SERVAUTH) RACLIST (SERVAUTH)
RDEFINE SERVAUTH (EZB.STACKACCESS.RA03.TCPIPA) UACC(NONE)
RDEFINE SERVAUTH (EZB.STACKACCESS.RA03.TCPIPB) UACC(NONE)
PERMIT EZB.STACKACCESS.RA03.TCPIPA ACCESS(READ) CLASS(SERVAUTH) ID(USER1)
PERMIT EZB.STACKACCESS.RA03.TCPIPA ACCESS(READ) CLASS(SERVAUTH) ID(USER2)
PERMIT EZB.STACKACCESS.RA03.TCPIPB ACCESS(READ) CLASS(SERVAUTH) ID(USER3)
SETROPTS CLASSACT(SERVAUTH) REFRESH RACLIST (SERVAUTH)
```

Uso do Controle de Acesso a Pilha

- **Negar o acesso de certos usuários ou grupos a uma pilha TCP/IP ou ao TCP/IP como um todo**
  - **Permite o controle de usuários de *shell* e *jobs batch***
- **Garante que servidores não se conectem a pilha TCP/IP errada**
  - **Cuidado: se o RACF negar o acesso de um servidor a uma pilha que ele esteja tentanto conectar, este servidor não será inicializado.**
- **Permite que um sistema se conecte seguramente a mais de uma rede TCP/IP**
  - **Pode garantir que as políticas de roteamente e firewall não foram contornadas**

Controle de Acesso a Porta TCP/IP

- **Os acessos as portas locais podem ser controlados por RACF**
- **São controlados por *profiles* na classe SERVAUTH**
- **Ativado por definições na PROFILE.TCPIP**
  - ***Keyword* SAF ativa o controle RACF na porta**
  - ***Keyword* RESERVED torna a porta totalmente indisponível (RACF não é invocado)**



Definições para Controle de Acesso a Portas

- PROFILE.TCPIP

```
PORT
      20 TCP OMVS       NOAUTOLOG  ; FTP Server
      21 TCP FTPDB1                ; FTP Server
      23 TCP * SAF TNPORT          ; Telnet Server
    2023 TCP OMVS                  ; Otelnetd
      25 TCP *                     ; Available to any user
     111 TCP RESERVED              ; Unavailable to any user
```

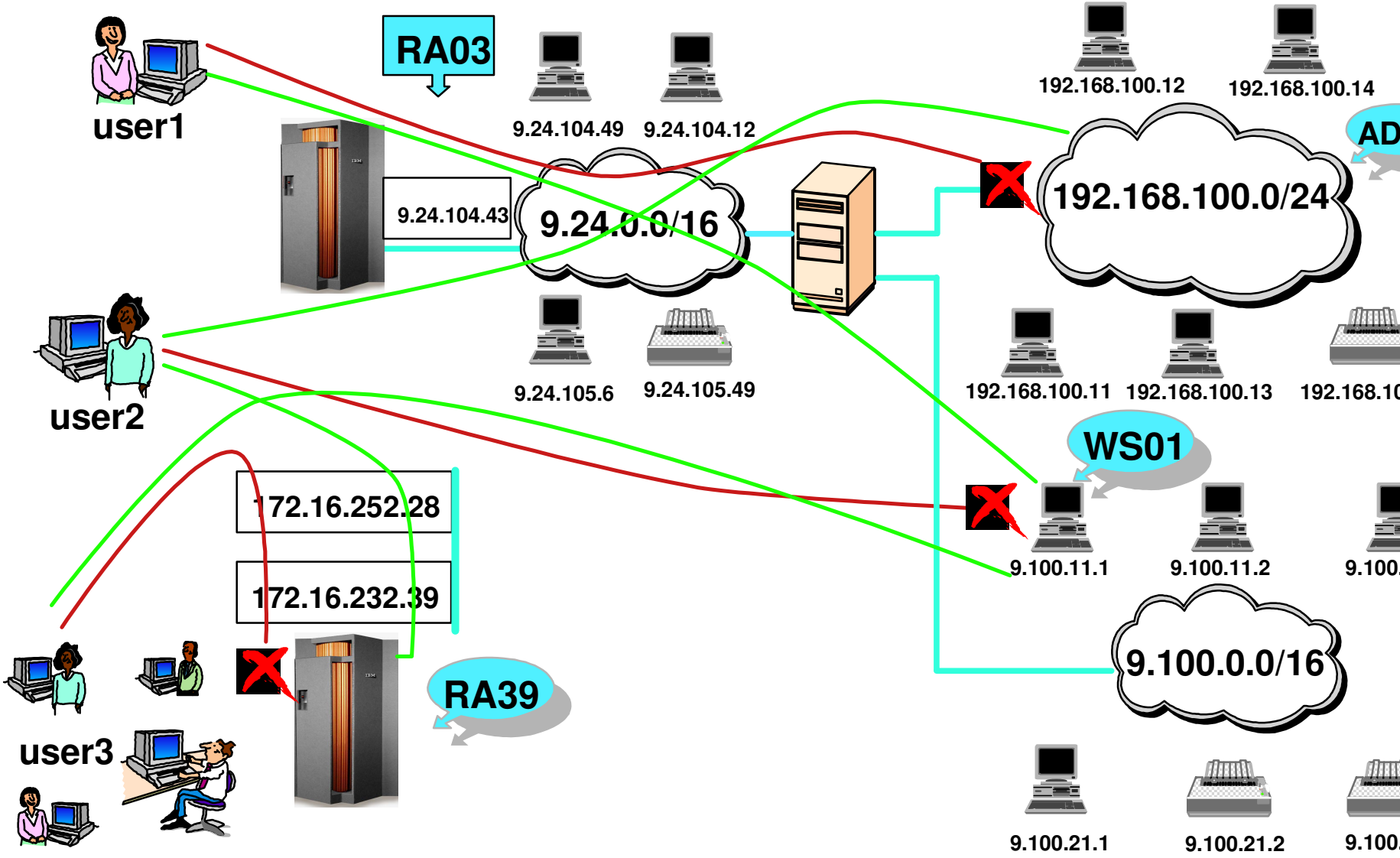
- RACF

```
SETROPTS CLASSACT(SERVAUTH) REFRESH
RDEFINE SERVAUTH (EZB.PORTACCESS.RA03.TCPIPB.TNPORT) UACC(NONE)
PERMIT EZB.PORTACCESS.RA03.TCPIPB.TNPORT ACCESS(READ) CLASS(SERVAUTH) ID(TCPIP2)
SETROPTS CLASSACT(SERVAUTH) REFRESH
```

Uso do Controle de Acesso a Portas

- Controlar o uso de portas por usuários do sistema local
- Pode ajudar no cumprimento da política de seguraça
  - Garante que serviços proibidos não rodem
- Mais seletivo que o controle de acesso a pilha TCP/IP
  - Usuários podem ser autorizados a utilizar somente portas específicas ou um *range* de portas
  - Serviços podem ser limitados aos usuários autorizados a acessá-los
  - Pode manter longe usuários bisbilhoteiros
- Pode prevenir a instalação de Cavalos de Tróia
  - Exemplo: Um servidor FTP falso que coleta usuário/senha de clientes

Controle de Acesso a Rede TCP/IP



Definições para Controle de Acesso a Rede

- PROFILE.TCPIP

num_mask_bits

```
NETACCESS
 ; Network              SAF
  192.168.100.0/24      ADM1
   9.100.11.1/32        WS01
   172.16.232.39/32     RA39
ENDNETACCESS
```

- RACF

```
SETROPTS CLASSACT(SERVAUTH) RACLIST(SERVAUTH)

RDEFINE SERVAUTH (EZB.NETACCESS.RA03.TCPIPB.ADM1) UACC(NONE)
RDEFINE SERVAUTH (EZB.NETACCESS.RA03.TCPIPB.RA39)  UACC(NONE)
RDEFINE SERVAUTH (EZB.NETACCESS.RA03.TCPIPB.WS01) UACC(NONE)

PERMIT EZB.NETACCESS.RA03.TCPIPB.WS01 ACCESS(READ) CLASS(SERVAUTH) ID(USER1)
PERMIT EZB.NETACCESS.RA03.TCPIPB.WS01 ACCESS(READ) CLASS(SERVAUTH) ID(USER3)
PERMIT EZB.NETACCESS.RA03.TCPIPB.ADM1 ACCESS(READ) CLASS(SERVAUTH) ID(USER2)
PERMIT EZB.NETACCESS.RA03.TCPIPB.RA39 ACCESS(READ)  CLASS(SERVAUTH) ID(USER2)

SETROPTS RACLIST(SERVAUTH) REFRESH
```

Uso do Controle de Acesso a Rede

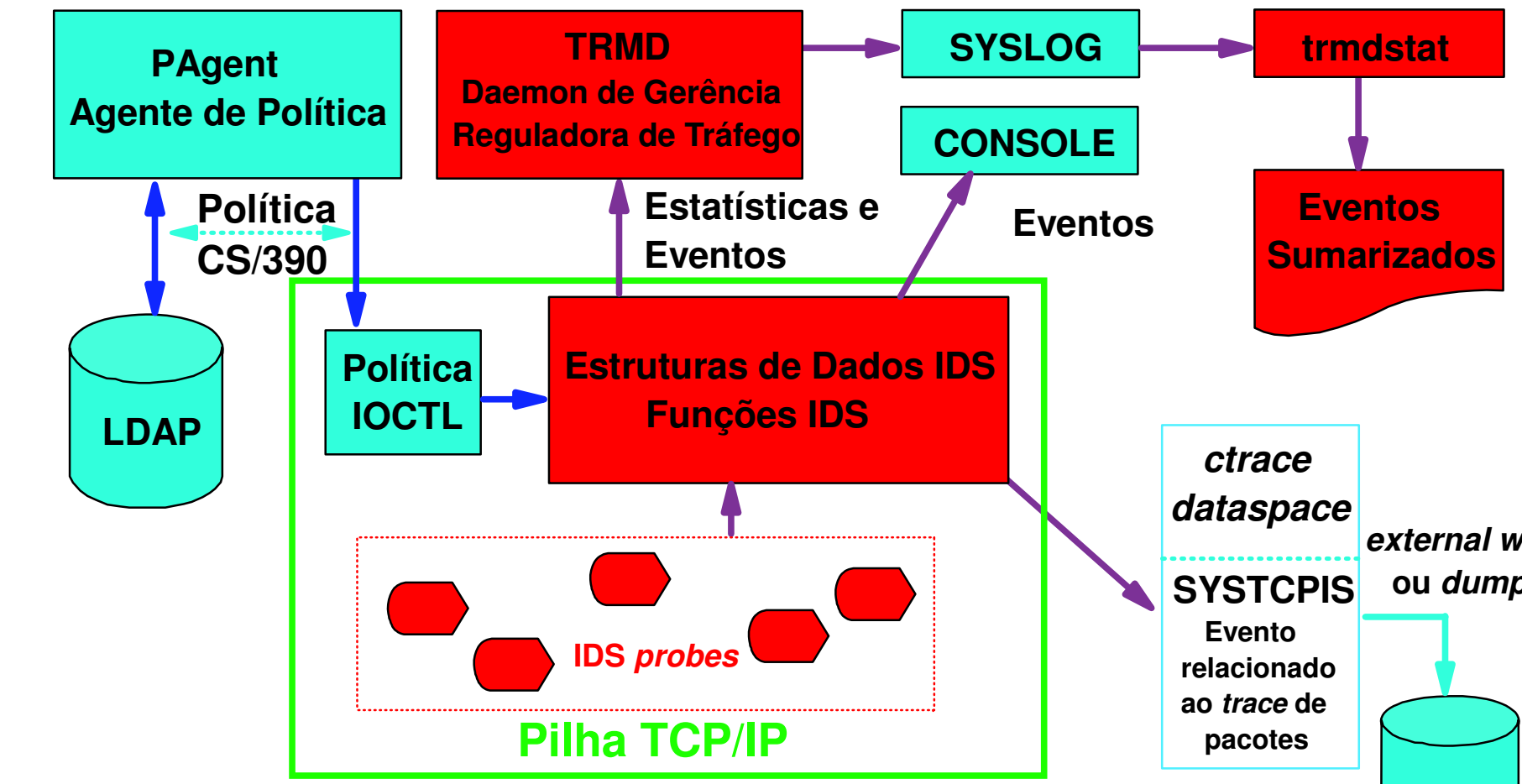
- **Permite que certas partes da rede sejam restritas a certos usuários**
- **Permite o controle de conexões de saída (*outgoing*)**
  - **SNA LU 6.2 controla somente conexões de entrada (*incoming*)**
- **Deve ser usado com cuidado para evitar um emaranhado de definições de controle**
- **Pode ser usado para proteger conexões servidor-a-servidor**
  - **Mas somente por um lado**
  - **Outras maneiras, como VPN, podem ser necessárias**
- **Pode ser usado para separar a intranet em zonas**
  - **Ajuda a limitar ataques de usuários internos**

Recomendações para TCP/IP

- **A IBM trabalha constantemente para melhorar a robustez da pilha TCP/IP no OS390**
  - **Geralmente, os *releases* mais recentes do OS/390 devem estar instalados para rodar servidores Internet**
  - **Mantenha o nível de manutenção atualizado**
- **O TCP/IP do OS/390 é testado contra ataques do tipo *denial-of-service* conhecidos**
  - **Isto é uma tarefa constante**
  - **Quando encontramos problemas, eles são corrigidos**
  - **A IBM não publica uma lista dos ataques testados**

Serviços de Detecção de Intrusão (IDS) z/OS V1R2

Serviços de Detecção de Intrusão (IDS)



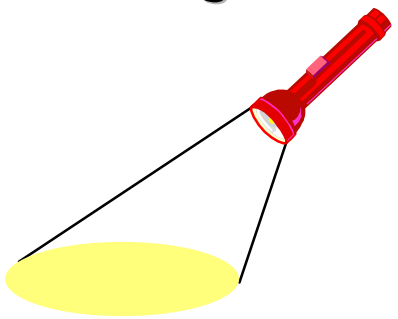
***Preview* do z/OS Versão 1 Release 2**

Introdução aos Serviços de Detecção de Intrusão

- **Os serviços de detecção de intrusão são controlados por políticas para identificar, alertar e documentar atividades suspeitas**
  - **As políticas de segurança estão centralizadas no diretório LDAP**
- **Integrado com a pilha TCP/IP**
- **Vantagens:**
  - **É capaz de avaliar dados IPSec de entrada (*inbound*)**
    - **Depois de decifrados no sistema receptor**
  - **Detecta anomalias estatísticas em tempo real**
    - **O sistema possui valores limite e declaração de dados sendo analisados**
  - **Políticas podem controlar os métodos de prevenção no sistema sendo avaliado**
    - **Limite de conexões, pacotes descartados**

Eventos dos Serviços de Detecção de Intrusão

- **Os Serviços de Detecção de Intrusão podem manipular as seguintes classes de eventos:**
  - **Detecção de *scan***
  - **Detecção de ataques**
  - **Detecção de *flood* e prevenção**



IDS: Detecção de *Scan*

- ***Scan* em portas TCP**
- ***Scan* em portas UDP**
- ***Scan* em ICMP**

O que é *SCAN* ?

- **Mapear os recursos da rede**
  - **Estrutura de *subnet*, endereços, máscaras**
  - **Endereços em uso, tipo de sistema, sistema operacional**
  - **Portas disponíveis, níveis de *release***

Definição de *Scan*

- **Os Serviços de Detecção de Intrusão definem um *scanner* como um sistema que acesse multiplos recursos (portas ou interfaces) durante um período de tempo.**
- **Duas categorias de *scans* são suportadas:**
  - ***Fast scan*** **- muitos recursos são rapidamente acessados em um curto período de tempo (geralmente menos de 5 minutos e executado por programa)**
  - ***Slow scan*** **- diferentes recursos são acessados intermitentemente durante um período de tempo longo (várias horas). Este pode ser um *scanner* tentando evitar ser detectado.**
- **Limite (recursos) e intervalo (período de tempo) podem ser especificados na política**

IDS: Detecção de Ataque

- **Verificação de um único pacote de entrada (*inbound*)**
  - **Verificação de pacote mal formado**
  - **Verificação de fragmento IP**
  - **Verificação de protocolo IP restrito**
  - **Verificação de opção IP restrita**
  - **Verificação de echo perpétuo em UDP**
  - **Restrições de redirecionamento ICMP**
- **Restrições de *outbound***
- **Proteção contra TCP Syn Flood**

IDS: Detecção de *Flood* e Prevenção

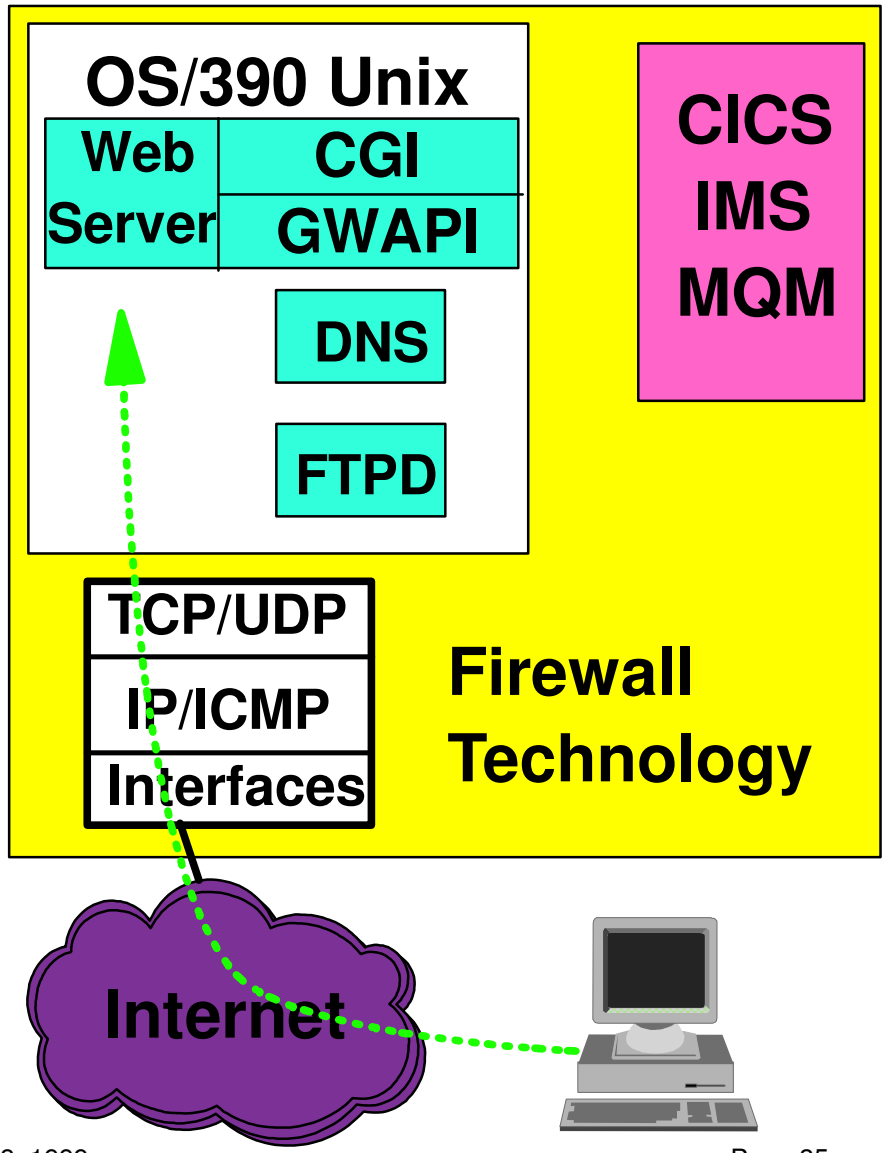
- **Propósito:**
  - **Detecção de *flood* e prevenção**
  - **Limitar o número de conexões e *address spaces***
- **Total de conexões TCP e gerenciamento do percentual por porta**
  - **Limitando conexões**
  - **Disponível no OS/390 V2R10**
- **Gerenciamento de *backlog* UDP por porta**
  - **Pacotes discartados**
  - **Limita o tamanho da fila de backlog por porta**

IDS: Opções de Reportes

- ***Log* de Eventos**
  - **Log de eventos suspeitos na console e/ou syslogd**
- **Estatísticas**
  - **Normal, exceção**
  - **Gravado na syslogd**
- ***Trace* de pacote após um ataque ser detectado**
  - **Para análise *offline***
  - **Documentação para ações legais**
  - **Independente do *trace* de pacote IP**

Uso do Serviço de Detecção de Intrusão

- **Usado para monitorar conexões da rede TCP/IP ao sistema z/OS**
- **Não deve ser utilizado para monitorar conexões roteadas**
  - **Não é efetivo quando o sistema z/OS é usado como um *firewall* de roteamento**



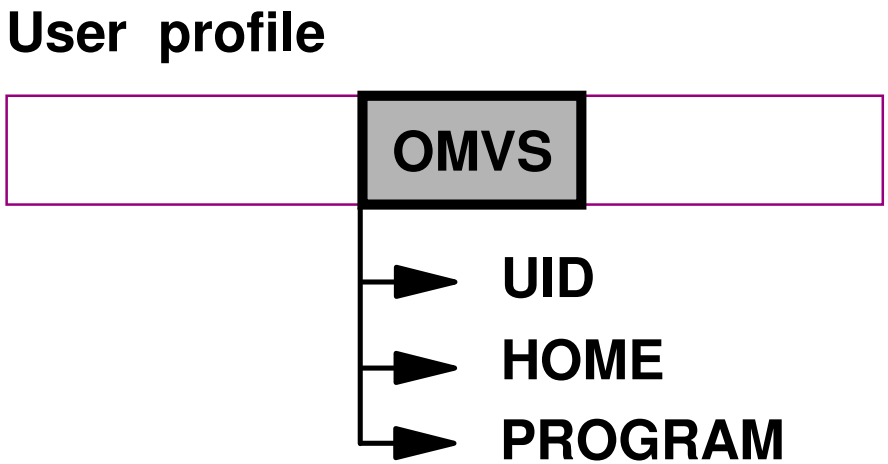
Protegendo o *Unix System Services* com RACF

OS/390 UNIX System Services

- UNIX environment integrated into OS/390
- Hybrid security mechanisms
  - UNIX UIDs and GIDs used as well as file permissions
  - Users and Groups defined in RACF, not in etc/security/passwd
  - Security services are performed by RACF
- UNIX security strengthened by RACF functions
  - SMF used for logging
  - Control of Superuser functionality
  - Control of security context switching
- Applications can use UNIX and MVS functions

RACF User Identification and Authentication

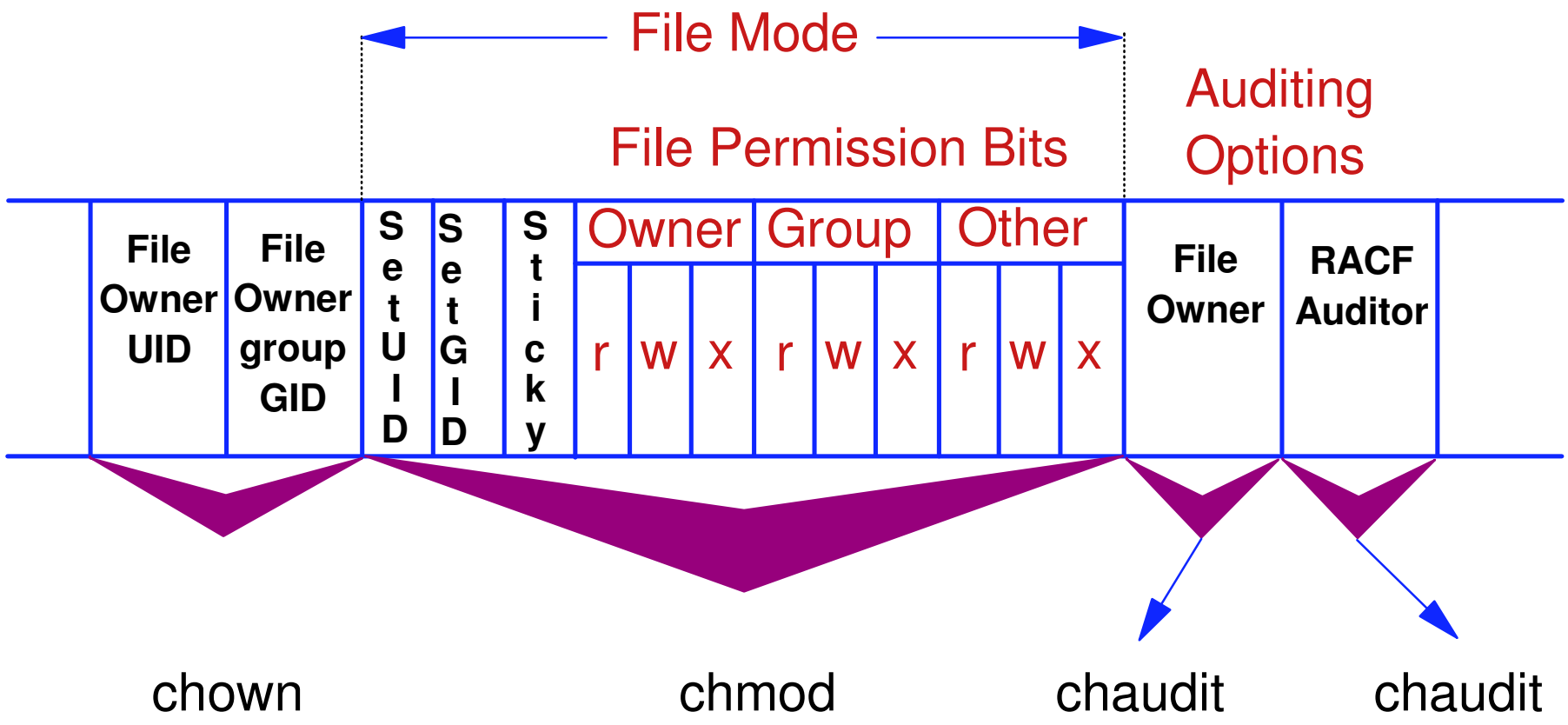
- **OS/390 UNIX user identification**
  - **RACF user profile with OMVS segment**
  - **RACF group profile with OMVS segment**
- **User authentication**
  - **RACF password**
- **OS/390 UNIX logon**
  - **TSO**
  - **r_login, telnet**



OS/390 USS HFS Files

- **Files in Hierarchical File System are not protected with RACF profiles**
  - **RACF classes for UNIX System Services resources exist, but are only used for global auditing options**
- **File Security Packet (FSP) contains permission bits**
  - **FSP for each file exists in directory (as in other UNIX systems where FSP is in INODE)**
  - **Access to file is not sufficient; user also needs access to directories from root down**
  - **When a file is created, FSP is created. UMASK determines permission bits in new FSP**

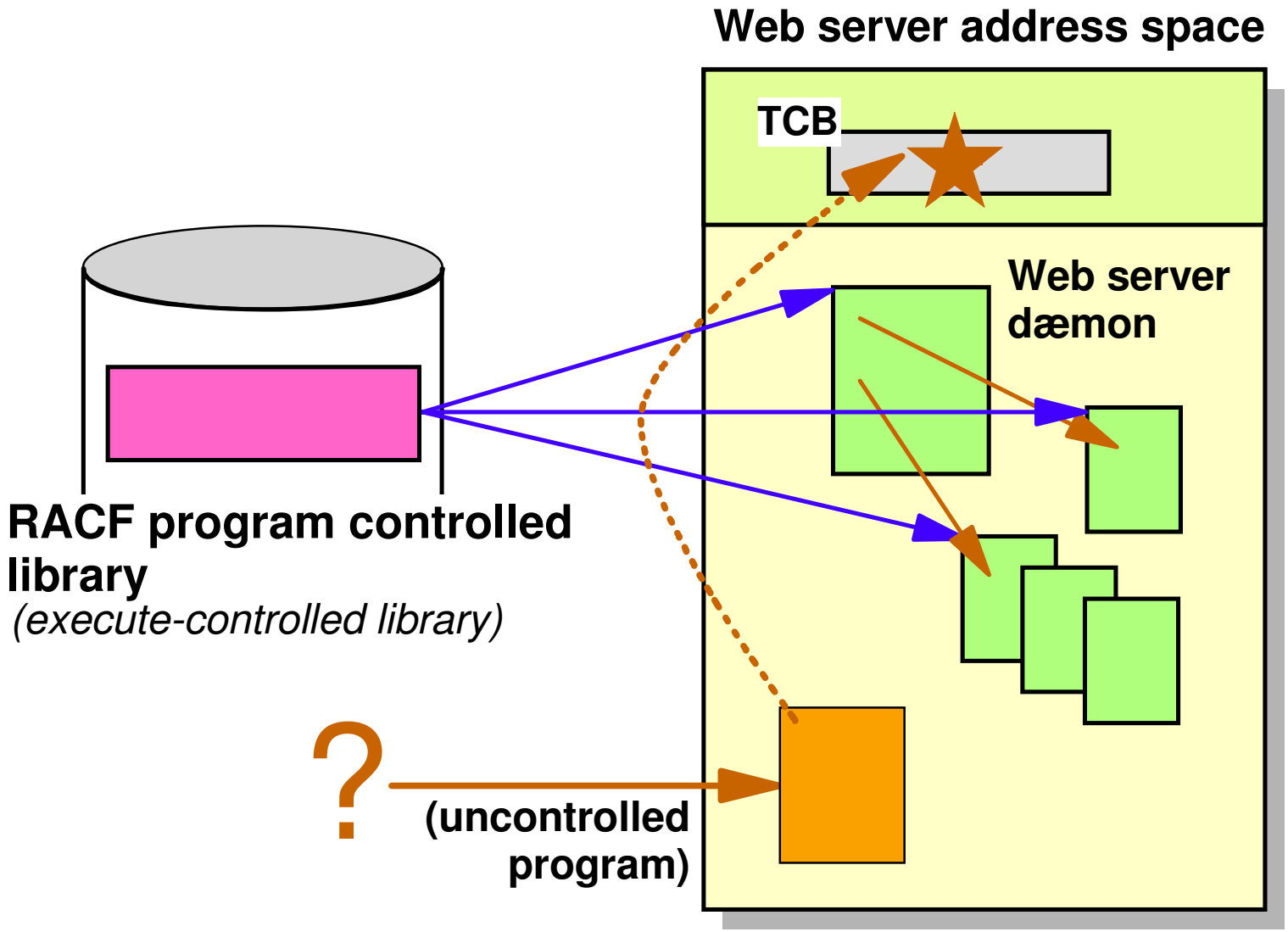
File Security Packet



OS/390 USS Use of Program Control

- **All programs needing daemon authority need to run in controlled environment**
  - **READ access to BPX.DAEMON in class FACILITY needed if service is called that changes UserId**
- **All modules in address spaces must**
  - **be loaded from MVS library (PDSE or PDS) defined in class PROGRAM, or**
  - **be loaded from HFS executable file with extattr +p defined**

Controlled Environment



Superusers

- In UNIX systems, superuser can access any file and switch to any other user's identity
- In OS/390 USS, superuser can access any file, but:
  - Superuser cannot switch into other user's identity without knowing user's password or SURROGAT authorization
  - Functions such as setting extended attributes require access to FACILITY class profile, not superuser
- Users with access to BPX.SUPERUSER can switch into superuser mode
  - Administrators and system programmers do not use UID=0 unless needed
  - Improved accountability
  - Supported by SMP/E since OS/390 V2R7

Superusers...

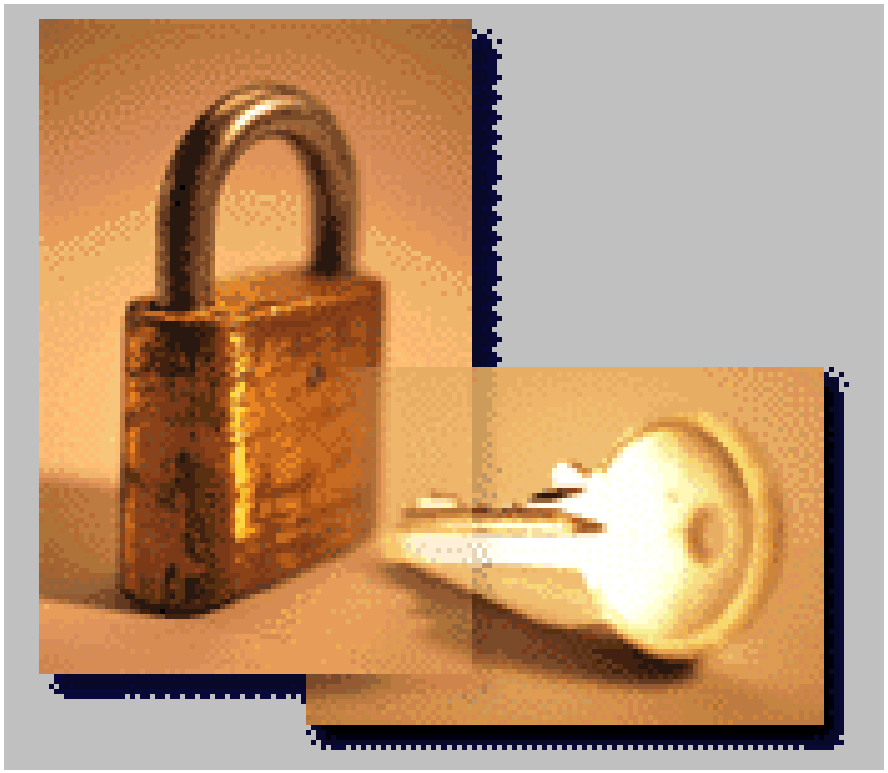
- **Functions otherwise requiring Superuser authority can be granted to normal users by permitting them to profiles in class UNIXPRIV**
  - **SUPERUSER.FILESYS**
  - **SUPERUSER.FILESYS.CHOWN**
  - **SUPERUSER.FILESYS.MOUNT**
  - **SUPERUSER.IPC.RMID**
  - **SUPERUSER.FILESYS.PFSCTL**
  - **SUPERUSER.PROCESS.GETPSENT**
  - **SUPERUSER.PROCESS.KILL**
  - **SUPERUSER.PROCESS.PTRACE**
  - **SUPERUSER.SETPRIORITY**
  - **SUPERUSER.FILESYS.VREGISTER**
  - **CHOWN.UNRESTRICTED**

RACF Control of Superuser Functions

- **Increased security by RACF control instead of superuser authority**
  - **BPX.FILEATTR.***
- **Less need for superuser authority through RACF control**
  - **Class UNIXPRIV**
- **Improved accountability by switching into superuser mode only when needed**
  - **BPX.SUPERUSER**

RACF Control of User Identity Changes

- **BPX.DAEMON**
  - ability to validate and assume RACF identities
  - dæmon programs can only change identity if authorized
- **BPX.SERVER**
  - surrogate assignment for POSIX threads
  - daemons can create threads with surrogate IDs if authorized:
    - UPDATE: client needs access authority to MVS resources
    - READ: client and server both need access authority



Cenário com zSeries na Internet

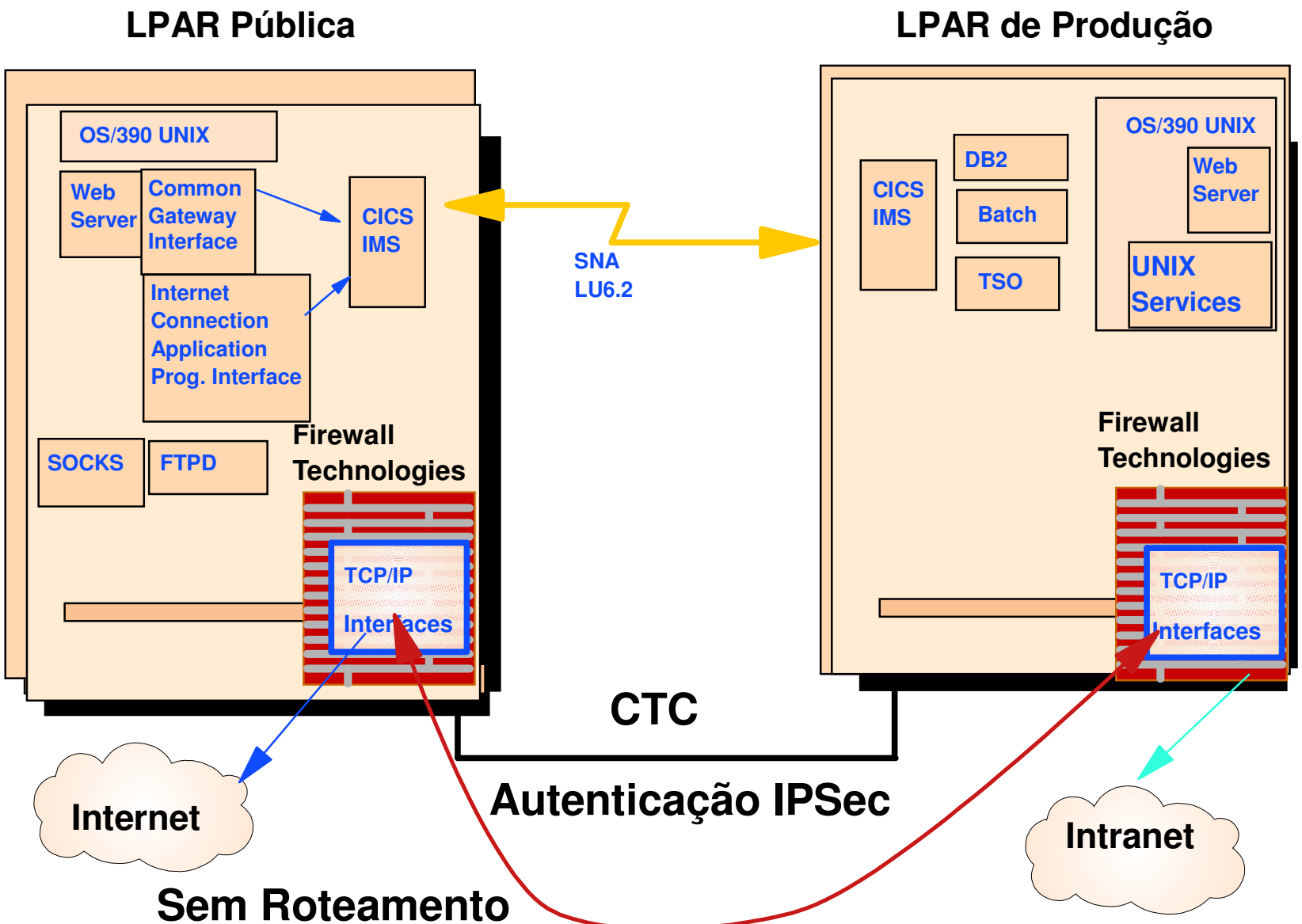
Autenticação na Web com RACF

- **Eu devo definir meus clientes externos no RACF ?**
  - **Principal ponto de decisão: O RACF será utilizado para autorizar o acesso de usuários a aplicações e recursos ?**
  - **Se não, então teremos pouco benefício em definirmos um grande número de usuários no RACF**
  - **Conexão a grupos não é mais um problema com z/OS V1R2**
    - **A função de grupos universais permite um número ilimitado de usuários conectados a um grupo**
  - **A autenticação do RACF pode ser feita em qualquer plataforma usando LDAP**
- **Um OS/390 HTTP server na DMZ pode compartilhar a base de dados RACF com sistemas de produção**
  - **Garanta que não exista usuários SPECIAL e OPERATIONS definidos com segmento OMVS**
  - **Não permita funções tais como o MVSDS *plugin***

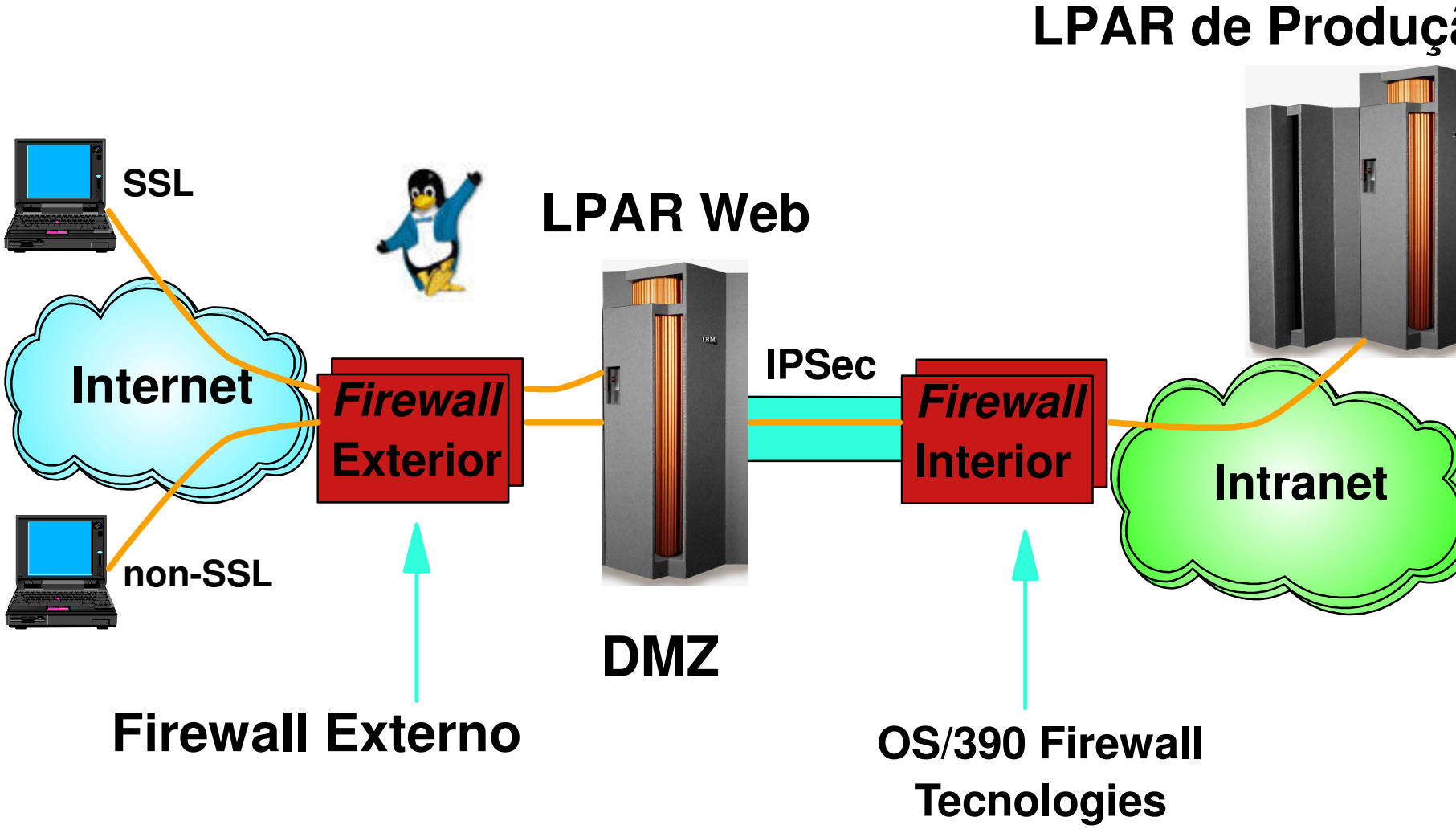
Comentários e Recomendações

- **IPSec pode ser usado para autenticar conexões**
  - **Previne que servidores não autorizados se conectem ao servidor de produção**
  - **IPSec não autentica usuários para aplicações**
- **Coloque um firewall externo entre a Internet e o zSeries**
  - **Alguns firewalls proporcionam funções que não estão disponíveis no OS/390 Firewall Technologies**
  - **Contudo, é recomendado utilizar o OS/390 Firewall Technologies como uma proteção adicional**

Cenário Exemplo de zSeries na Internet



Versão zSeries de uma DMZ



Perguntas ?