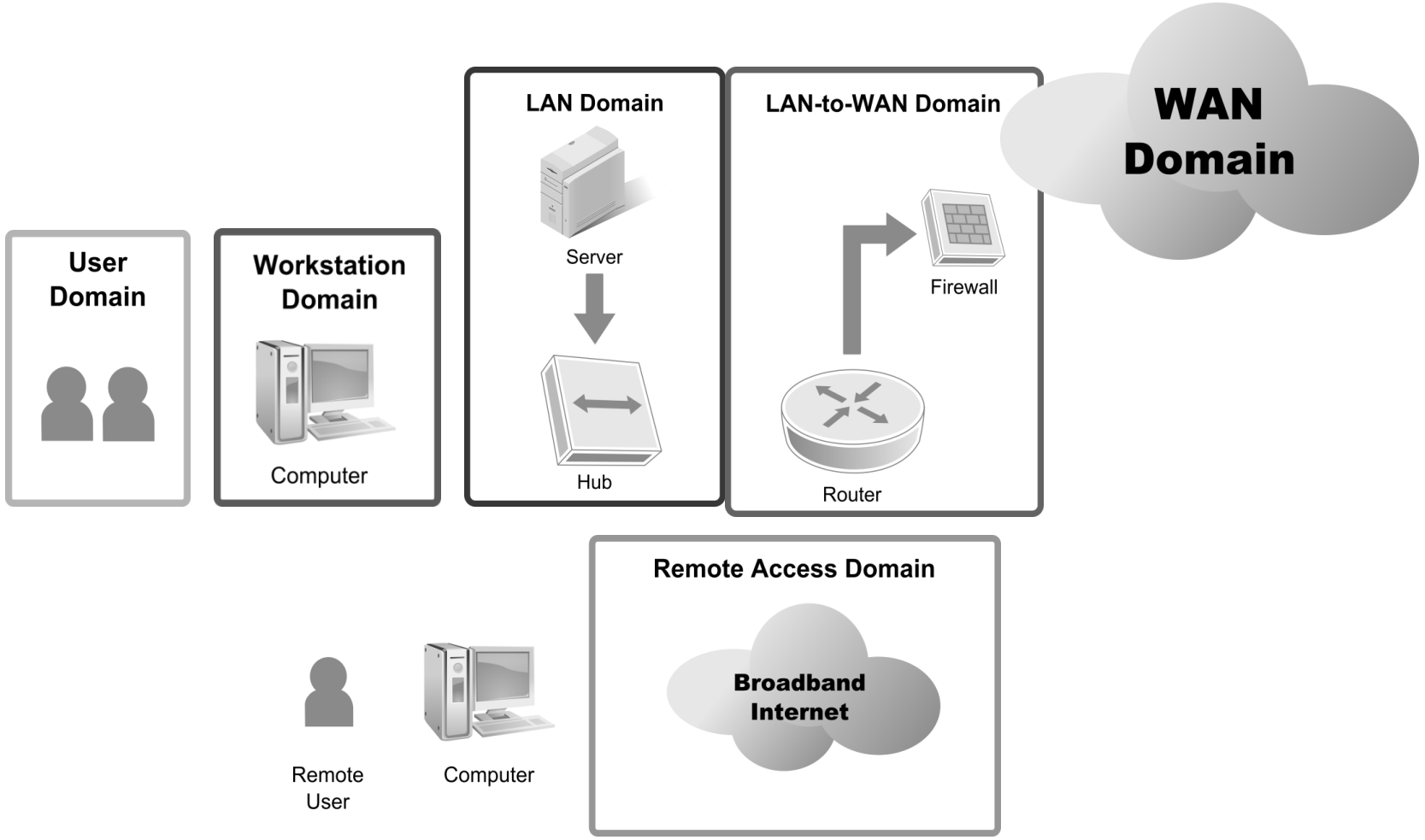
Segurança de Ambientes com uso da TI

Prof. Dr. Lauro Cássio Martins de Paula

lauro.martins@ifba.edu.br

Domínios de uma infraestrutura de TI

Domínios de uma infraestrutura de TI



Kim & Solomon,2014.

Domínios de uma infraestrutura de TI

- Domínio de usuário;
- Domínio de estação de trabalho;
- Domínio de LAN;
- Domínio de LAN para WAN;
- Domínio de WAN;
- Domínio de sistema/aplicativo;
- Domínio de acesso remoto.

Tipos de Ameaças

Ameaças comuns no domínio do usuário

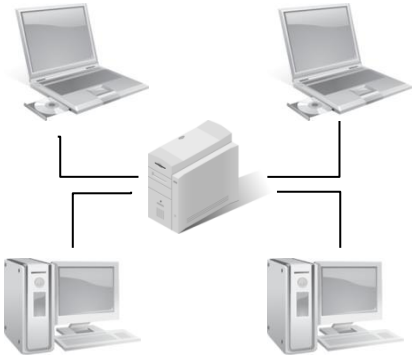
1. Falta de conscientização do usuário
2. Apatia dos usuários com as políticas
3. Violações de políticas de segurança
4. Usuários inserem cd/dvd/usb etc com arquivos pessoais.
5. Download de arquivos
6. Usuário descontente faz uso de sabotagem
7. Perda de interesse de funcionário
8. Chantagem ou extorsão de funcionário

Ameaças comuns no domínio da estação de trabalho

1. Acesso não autorizado à estação de trabalho
2. Acesso não autorizado a sistemas, aplicativos e dados
3. Vulnerabilidade do SO
4. Vulnerabilidade através de atualizações de softwares
5. Infecção por vírus, código malicioso, etc.
6. Download de arquivos

Ameaças comuns no domínio da LAN

1. Acesso não autorizado à LAN
2. Acesso não autorizado a sistemas, aplicativos e dados
3. Vulnerabilidade de sistemas, softwares
4. Servidores com diferentes Hw's, SO's e SW
5. Confidencialidade de dados comprometida



Ameaças comuns no domínio da LAN para WAN

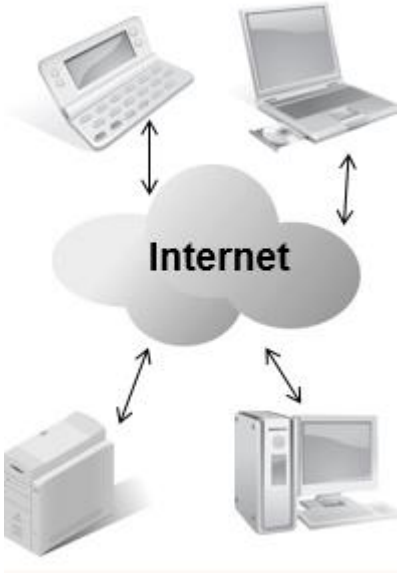
1. Sondagem e varredura de porta de rede sem autorização
2. Acesso não autorizado
3. Vulnerabilidade no roteador, firewall, etc..
4. Usuários locais fazem download de arquivos desconhecidos em fontes desconhecidas

Ameaças comuns no domínio da WAN

1. Aberta, pública e acessível a qualquer um.
2. Boa parte do tráfego da internet é enviada em texto claro
3. Vulnerável a ataques maliciosos
4. Vulnerável a ataques de negação de serviços
5. Vulnerável a adulteração de dados e informação
6. Aplicativos TCP/IP são inerentemente inseguros
7. Hacker, invasores enviam livremente vírus, código malicioso, etc por e-mail.

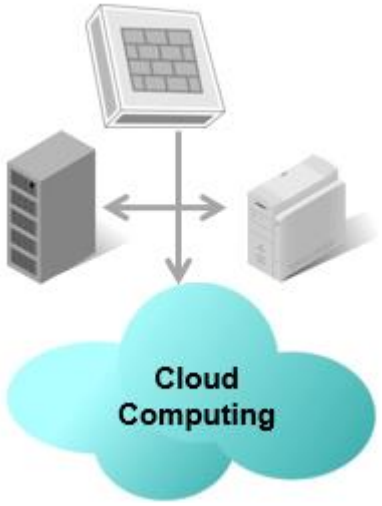
Ameaças comuns no domínio de acesso remoto

1. Ataques de ID e de senha do usuário
2. Múltiplas tentativas de acesso e ataques a controle de acesso
3. Acesso remoto não autorizado a sistemas de TI, aplicativos e dados
4. Dados confidenciais são comprometidos remotamente
5. Vazamento de dados
6. Laptop de trabalhador móvel é roubado



Ameaças comuns no domínio de sistema/Aplicativos

1. Acesso não autorizado a data centers, sala de computadores e gabinetes de fiação
2. Dificuldade em gerenciar servidores que requerem alta disponibilidade
3. Vulnerabilidade de SO do servidor
4. Dados perdidos ou corrompidos



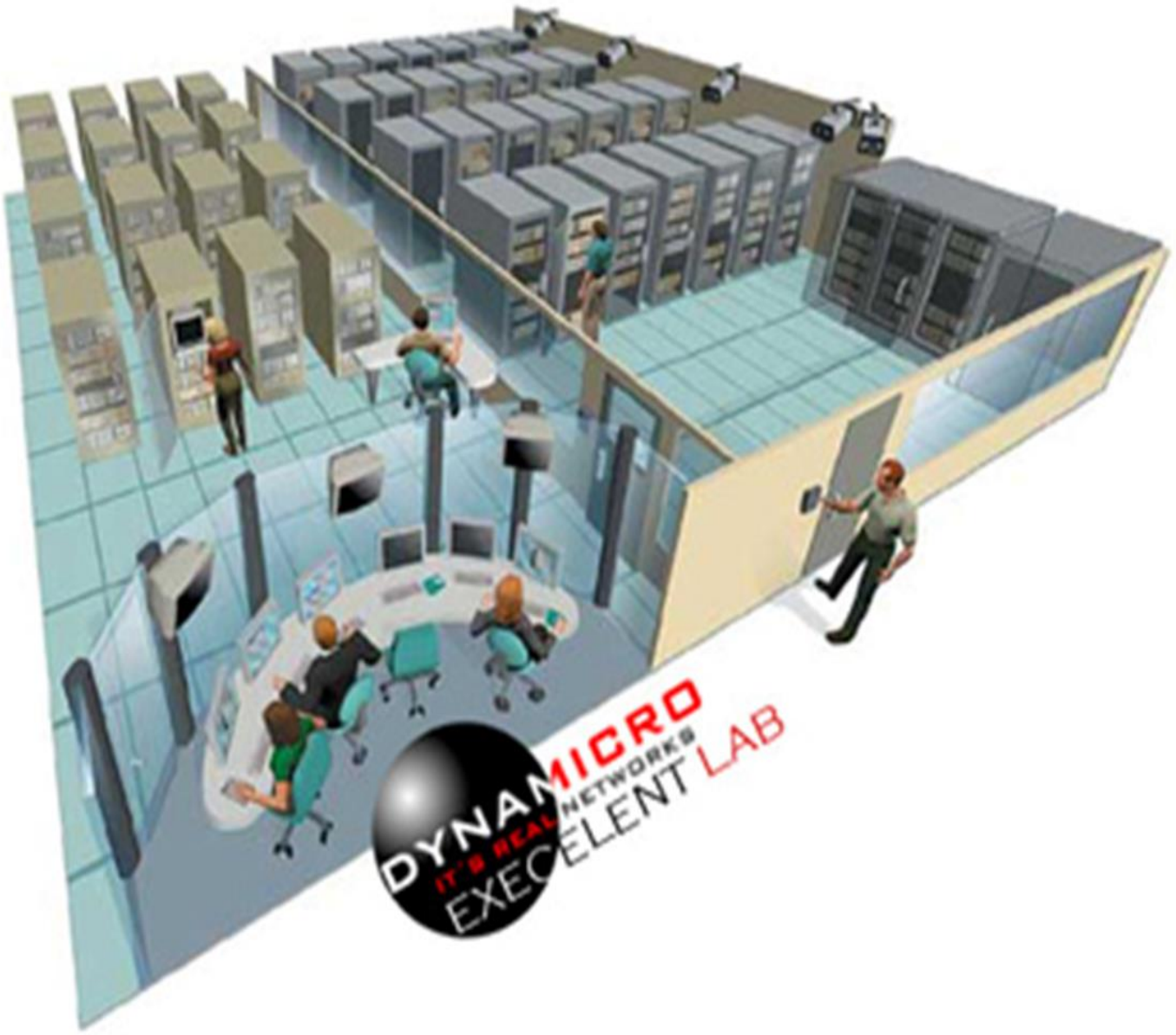
Segurança de Ambiente em uma Infraestrutura de TI

Segurança do Ambiente

- Para garantir adequada segurança de um ambiente, é necessário combinar as seguintes medidas:
  - De prevenção;
  - Detecção; e
  - Reação aos possíveis incidentes de segurança.

- Algumas normas (**ISO 27.002**) tratam das seguintes medidas de ***controle de acesso***:
  - **Físicas** - muros, cercas, trancas, etc.
  - **Lógicas** - sistema de login, etc.
  - **Combinação de ambas** - tokens, etc.

Controle de Acesso



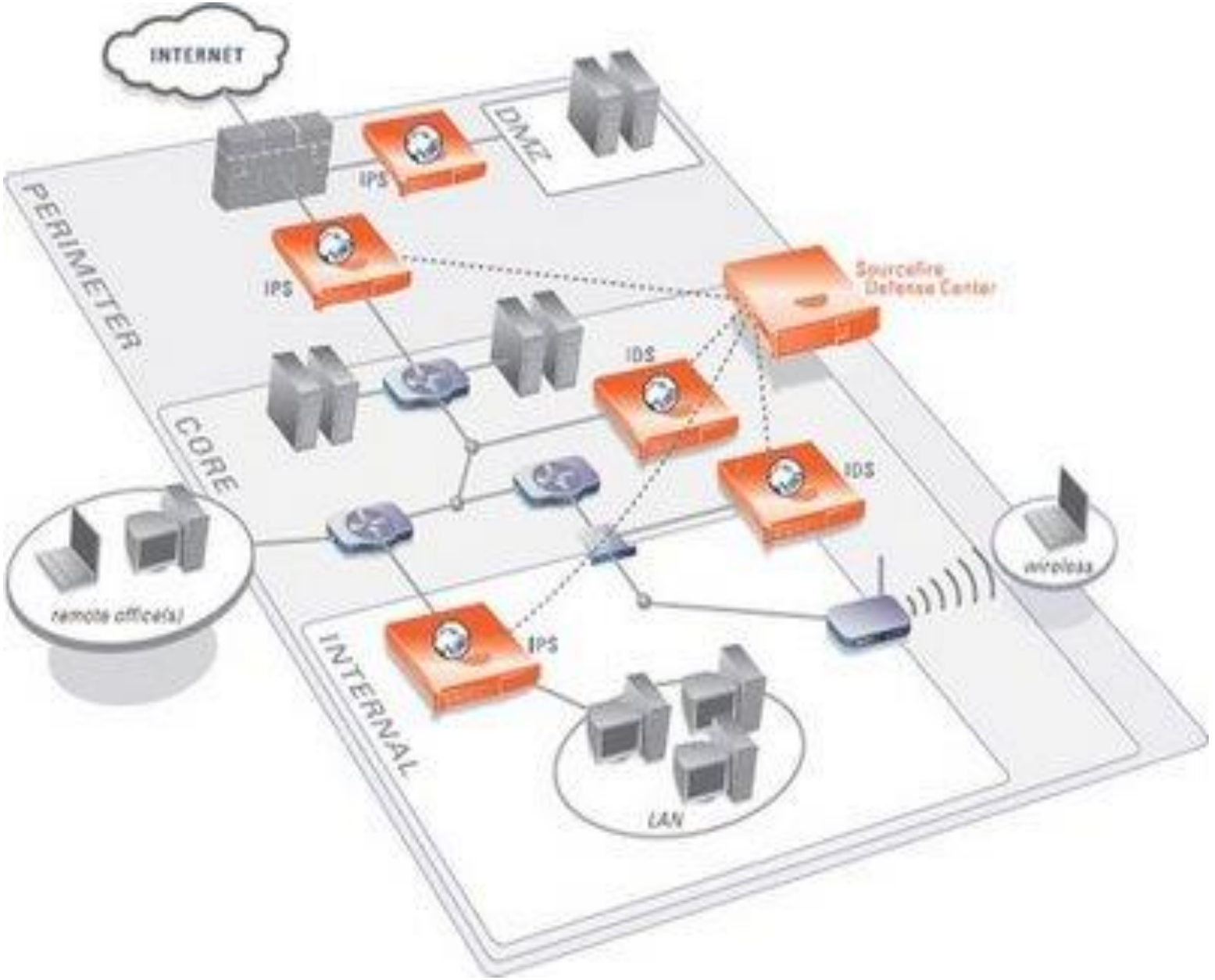
Controle de Acesso

O controle de acesso pode ser dividido em controle lógico ou físico onde temos:

- **Controle Lógico**
  - Identificação e autenticação do usuário;
  - Administração dos privilégios de usuários;
  - Monitoramento de uso e acesso ao sistema.

- **Controle Físico**
  - Controles de entrada apropriados;
  - Implantação de dispositivos de segurança.

Segurança do Ambiente Físico



Segurança do Ambiente Físico

Perímetro de Segurança:

- É o contorno ou linha imaginária que delimita uma área ou região separada de outros espaços físicos por um conjunto qualquer de barreiras.

- A definição clara do perímetro de segurança ajudar a estabelecer melhor os investimentos e definir que tipos de barreiras são mais adequadas para a proteção do **ativo da informação.**

Segurança do Ambiente Físico

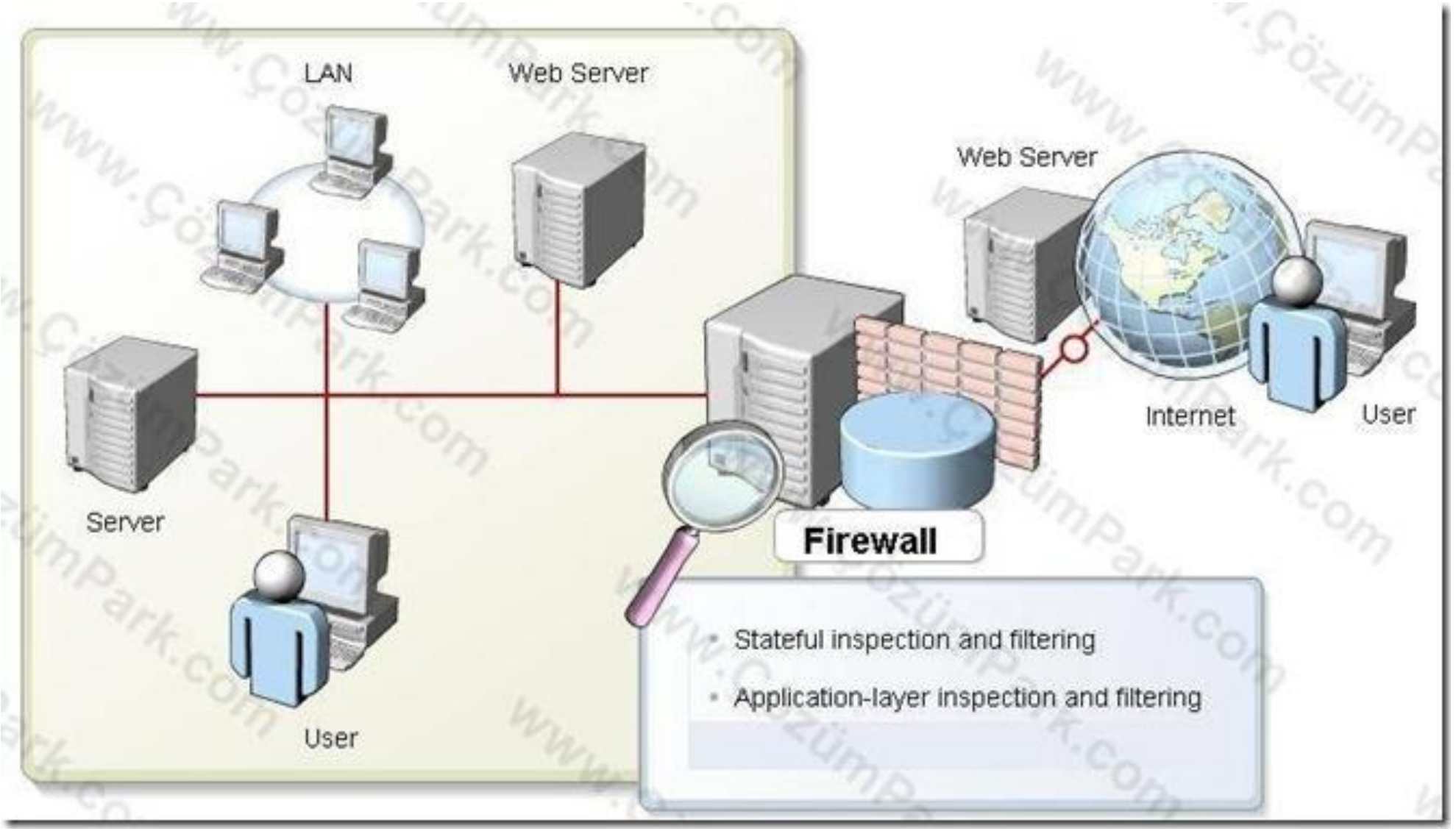
Perímetros a serem protegidos podem ser:

- Prédios;
- Geradores;
- Casas;
- Indústrias.

O que deve ser controlado:

- Documentos em papel;
- Equipamentos;
- Escritórios.

Segurança do Ambiente Lógico



Segurança do Ambiente Lógico

- **Segurança em Redes**;
  - Autenticação e restrição de acesso;
- **Firewalls**;
  - Barreira de proteção para controle de acesso;
- **Perímetros lógicos**;
  - VPN;
- **Antivírus**;
- **Criptografia**;
- **Assinatura digital**;
- **Certificado digital**.

***Cada grupo deve escolher um destes tópicos para falar no seminário!**