Capítulo ...

Pensando em
Política de Segurança de Rede

Objetivos deste capítulo

- Identificar a finalidade de uma política de segurança.
- Identificar os componentes de uma política de segurança de rede.
- Identificar como implementar uma política de segurança de rede.
- Avaliar a política de segurança de rede da Empresa XYZ.

Introdução

- Avaliação de uma política de segurança de rede numa empresa corporativa.
- Economia ao proteger a rede.
- Equilíbrio entre o nível de segurança necessário e a facilidade de uso para que o usuário obtenha a segurança de rede ideal.

Importância de proteger a rede

- Ao analisar uma política de segurança deve-se comparar o custo referente aos recursos humanos e de capital para implantar a política, com os custos de exposições a violações de segurança.

Importância de proteger a rede

- O **investimento na segurança da rede** deve ser comparado com o **possível prejuízo econômico a possíveis violações de segurança**.

Avaliação dos Custos

- Determine o custo único e de ciclo de vida de cada controle de segurança.

  O ciclo de vida da maioria dos HW relacionados a computador é três a cinco anos.

Avaliação dos Custos

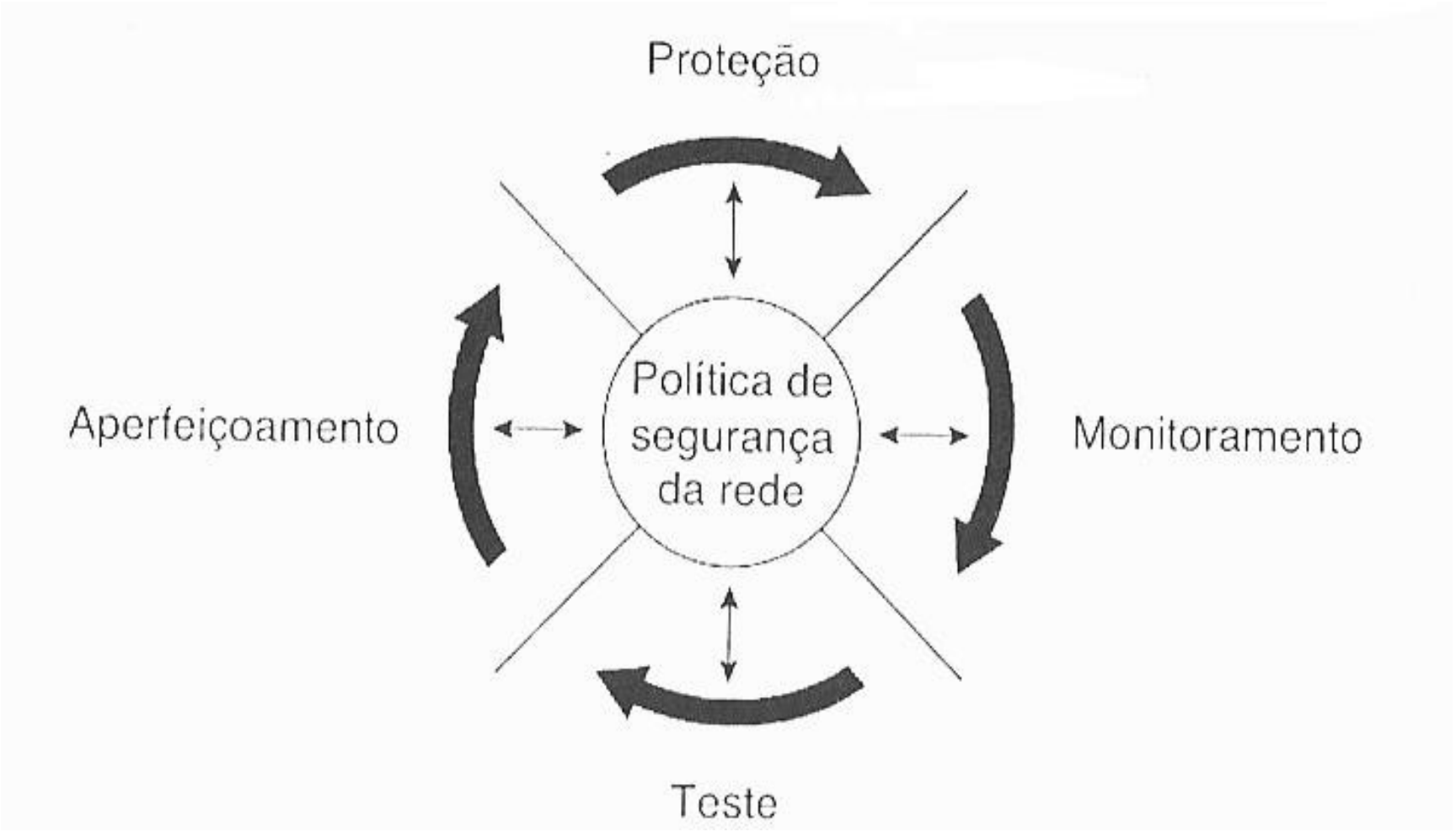
- Identifique a redução da exposição a danos se os controles de segurança forem implementados.
- Identifique o dano máximo possível se os controles de segurança não forem implementados.

Avaliação dos Custos

- Determine a economia de vida útil que os controles de segurança permitirão.

- Decida quais controles são mais vantajosos e econômicos.

Processo para implementar segurança



Avaliando a postura de segurança

- É o esforço contínuo e iterativo da empresa para tentar proteger seus bens mais importantes, da maneira mais econômica, reduzindo o risco a um nível aceitável.

Processo para implementar segurança

- Proteção
- Monitoramento
- Teste
- Aperfeiçoamento

Proteção

- Proteger os dados corporativos no nível necessário.
- Tecnologias de segurança são implantadas.
- Firewalls, sistemas de autenticação, proxy Web, sistemas de detecção de intrusão, protocolos criptografados.

Monitoramento

- Observar a atividade em pontos críticos de acesso à rede.
- Monitorar continuamente a rede para verificar intrusões.

Teste

- Certificar-se de que as medidas de segurança sejam suficientes para resistir à sofisticação crescente e freqüência de ataques.

- Como as redes mudam com freqüência, é necessário testar sua postura de segurança e fazer avaliações das vulnerabilidades.

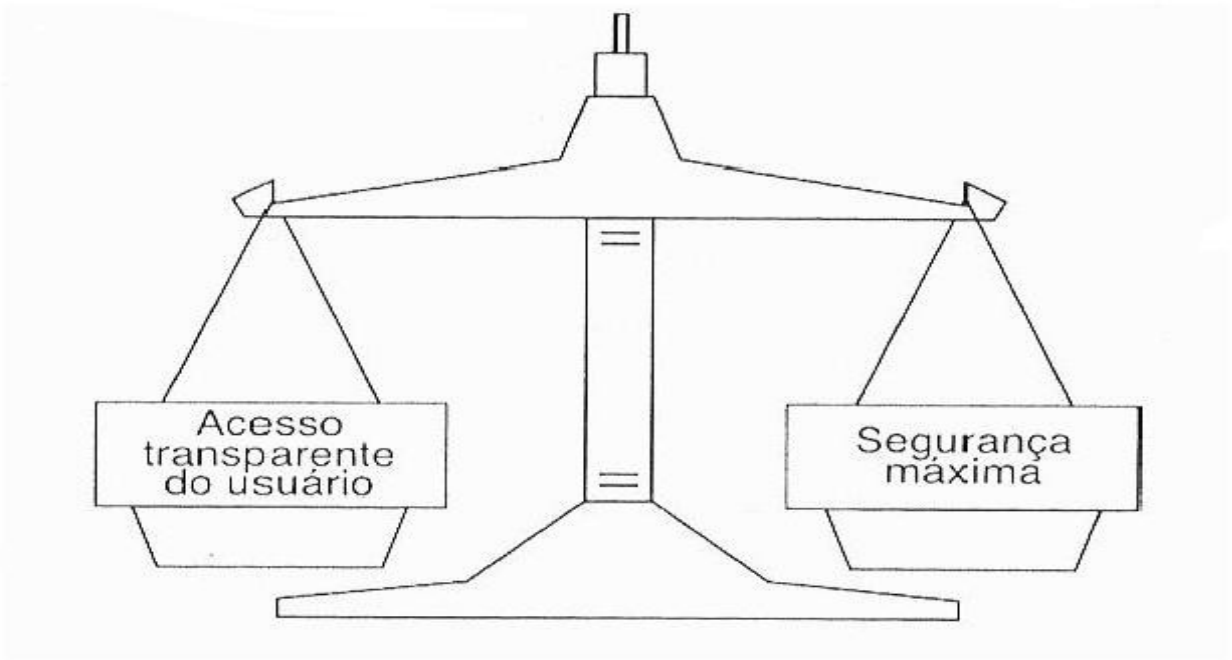
Aperfeiçoamento

- Atualizar as medidas de segurança conforme necessário.
- Atingir o máximo de eficiência operacional e implementar rapidamente os aperfeiçoamentos.

Chave para implantar com êxito a segurança da rede

- Equilibrar a facilidade de uso com o nível de segurança apresentado pelas medidas.
- Se os custos de segurança forem desproporcionais em relação aos riscos reais, haverá prejuízo para a empresa.
- Se as medidas forem restritivas demais, os usuários poderão encontrar meios de alterá-las.

Chave para implantar com êxito a segurança da rede



Avaliando uma política

- A parte mais importante do controle da segurança da rede consiste em implementar a política de segurança.
- Analisar a política e, depois, implementá-la na rede real.

O que é uma Política de Segurança?

- "**Política de segurança** é uma declaração das regras que devem ser obedecidas pelas pessoas que têm acesso à tecnologia e às informações de uma empresa."

  - Site Security Handbook (RFC 2196)

O que é uma Política de Segurança?

- “Uma **política de segurança** é um documento que resume como uma corporação usará e protegerá seus recursos computacionais e de rede.”

Porque se deve criar ...

- Fornece uma estrutura de segurança geral para implementar a segurança.
- Define qual comportamento é permitido ou não.
- Determina quais ferramentas e procedimentos são necessários.
- Define as responsabilidades dos usuários e administradores.

Porque se deve criar ...

- Ajuda a comunicar o consenso em um grupo de pessoas de decisões.
- Define um processo para tratar os incidentes de segurança.
- Permite a imposição da segurança global.
- Fornece um processo para se fazer auditoria da segurança.
- Cria uma base para ação legal, se necessário.

O que deve conter

- Declaração de autoridade e escopo.
- Política de uso aceitável.
- Política de autenticação.
- Política de acesso à Internet.
- Política de acesso remoto.
- Procedimento de tratamento de incidentes.

Como usar uma política: algumas maneiras

- Identificando bens e ameaças.
- Determinando a implementação
- Educando os usuários.

Auditorias regulares

- Fornecem um visão geral do estado de segurança.
- Testar as medidas de segurança contra invasões.
- Detectar atividades ilícitas de funcionários.
- Usar ferramentas para auditorias.

Ferramentas de auditoria

- Scanner CiscoSecure
- COPS (Computer Oracle and Password System)
- Tiger
- TARA (Tiger Analytical Research Assistant)
- Tripwire
- Simple WATCHdog (Swatch)

Scanner CiscoSecure

- Auditoria da postura de segurança de uma rede através do exame de mapeamentos e vulnerabilidades da rede.
- Facilita o gerenciamento de riscos através do acesso imediato a dados de vulnerabilidade.
- Windows ou Solaris.

COPS

- Inspeção de segurança que verifica se sistemas UNIX estão configurados para serem menos vulneráveis a ataques remotos.

Tiger e TARA

- Scripts UNIX para verificar vulnerabilidades nos sistemas UNIX.
- Filtragem de pacotes.
- Programa de verificação de configuração.
- Programa de auditoria baseada em log.
- TARA é uma atualização de Tiger para UNIX e Linux.

Tripwire

- Monitor de integridade do sistema de arquivos UNIX, se arquivos-chave foram alterados.
- Ferramentas derivadas:
  - ViperDB
  - Triplight
  - AIDE (Advanced Intrusion Detection Environment)
  - Sentinel

Swatch

- Analisador de *logs* para sistemas UNIX que procuram eventos específicos em *logs* de evento.

- Versões shareware de cada ferramenta:
  - http://www.rootshell.com

Melhorando a postura de segurança

- Manter-se atualizado sobre novos ataques e vulnerabilidades de rede: grupos de notícias, eventos sobre segurança e publicações.
- Listas de e-mail relativas à segurança.
- Sites Web: http://www.sans.org
  http://www.securityfocus.com
  http://www.cert.org

Melhorando a postura de segurança

- Manter-se atualizado quanto a novas tecnologias e técnicas de segurança para proteger equipamentos.
- Observe sites de fornecedores para anúncios sobre *patches* e novas versões.
- Teste e instale *patches* de segurança para correção de erros.

Melhorando a postura de segurança

- Forneça treinamento contínuo sobre conhecimento de segurança e mantenha fluxo de informações para grupos.
- Implemente novas tecnologias de segurança.
- Avalie produtos no ambiente de laboratório, antes de instalá-los.

Melhorando a postura de segurança

- Fazer análises regulares de perfis de ataque.

  Por exemplo, um IDS pode conter um BD de segurança de rede e uma lista de assinaturas de ataques.

  Essa lista é atualizada regularmente e deve ser aplicada ao IDS.

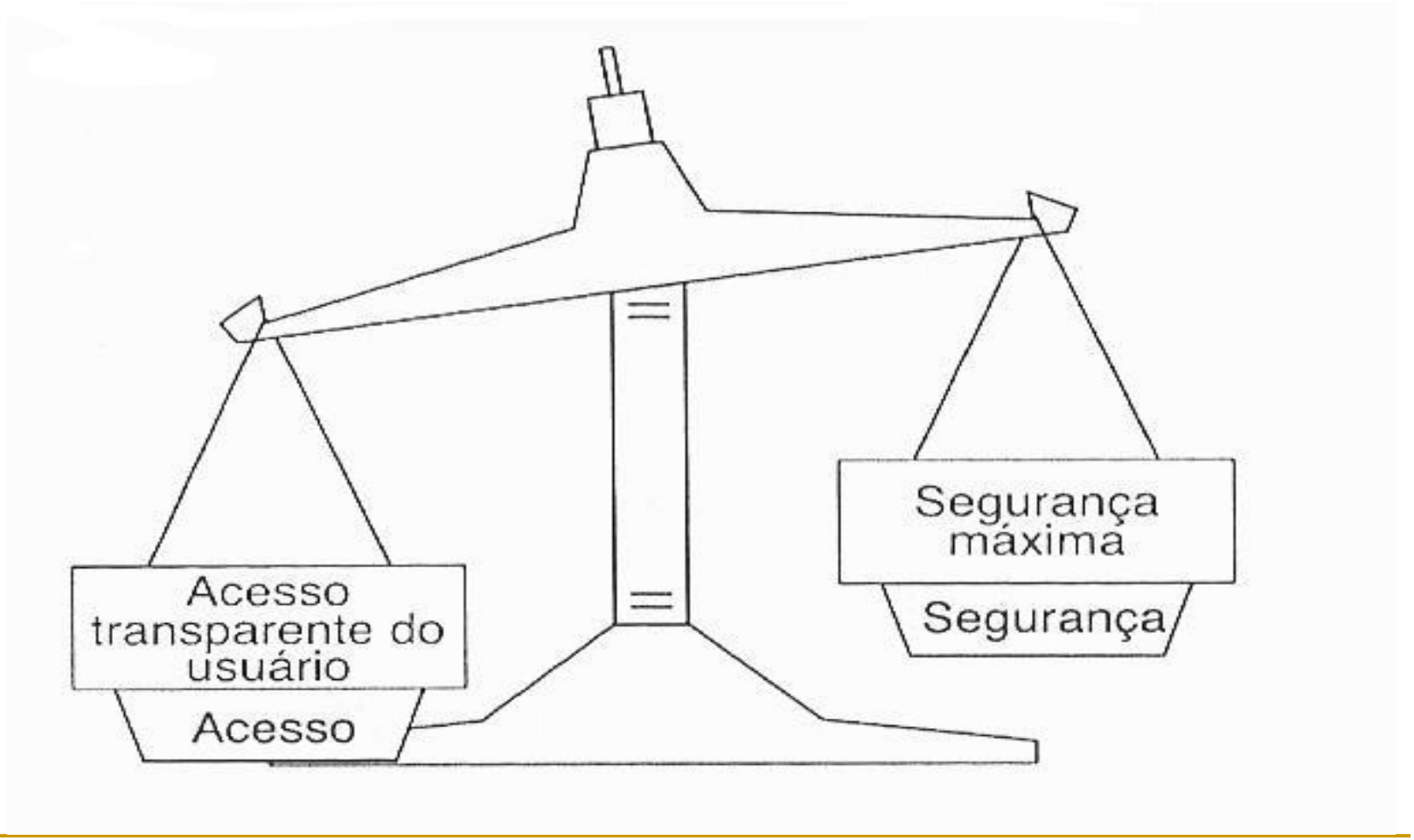
  O BD fornece acesso imediato a informações sobre ataques e medidas defensivas.

Melhorando a postura de segurança

- Reconfigure a rede conforme necessário, com base na análise dos perfis de ataque.
- Proporcione investigação, relatórios e acompanhamento de incidentes de segurança.
- Atualize as políticas e procedimentos de segurança da empresa.

Classificando as políticas de segurança

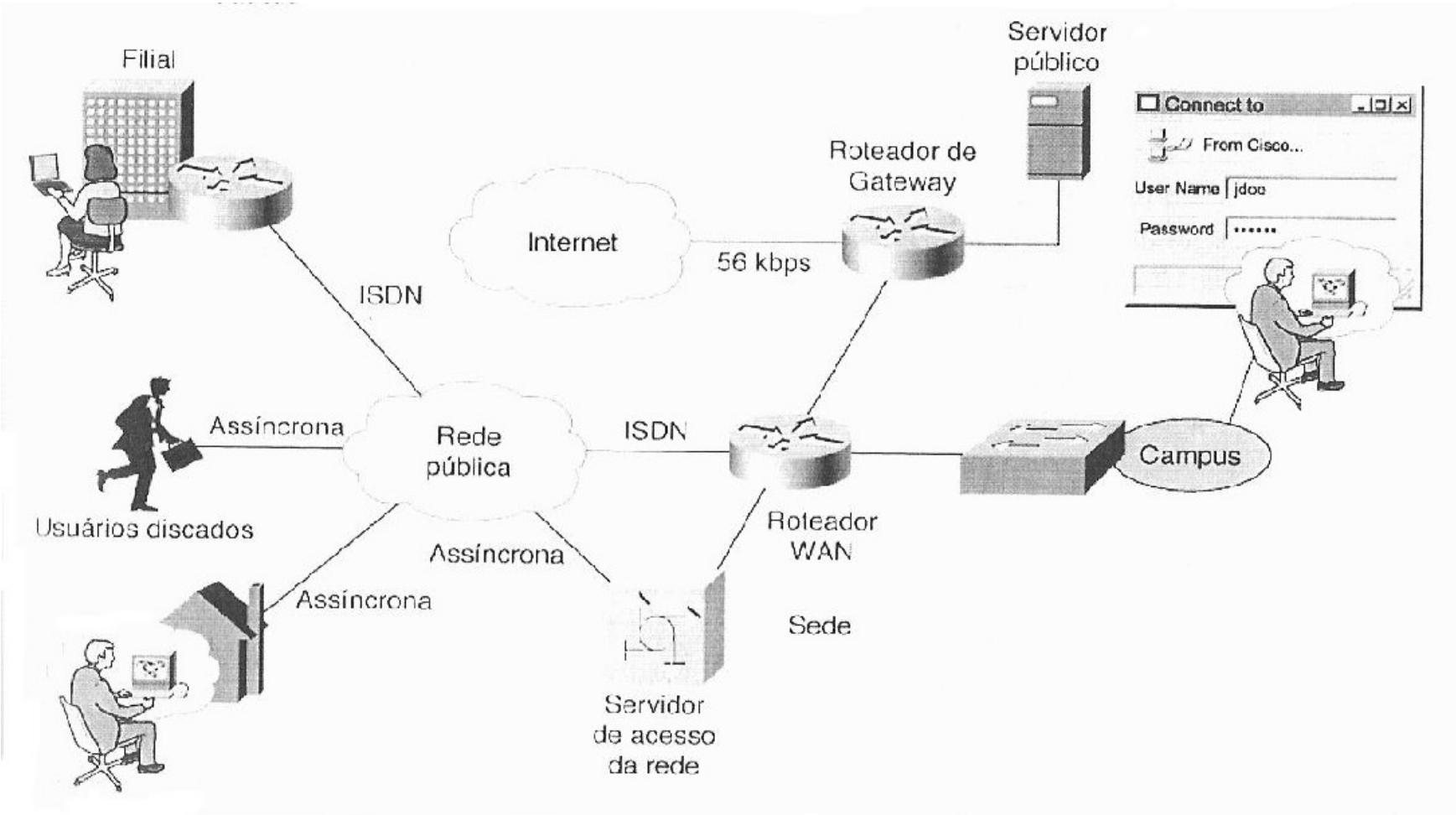
Estudo de Caso 1 – Política de Segurança Aberta (Mínima)



Estudo de Caso 1 – Política de Segurança Aberta (Mínima)

- Permitir tudo o que não for explicitamente proibido.
- Fácil de configurar e administrar.
- Fácil para usuários da rede.
- Custo da segurança:
  - US$ 70,00 por computador.

Estudo de Caso 1 – Ambiente de rede para Segurança Mínima

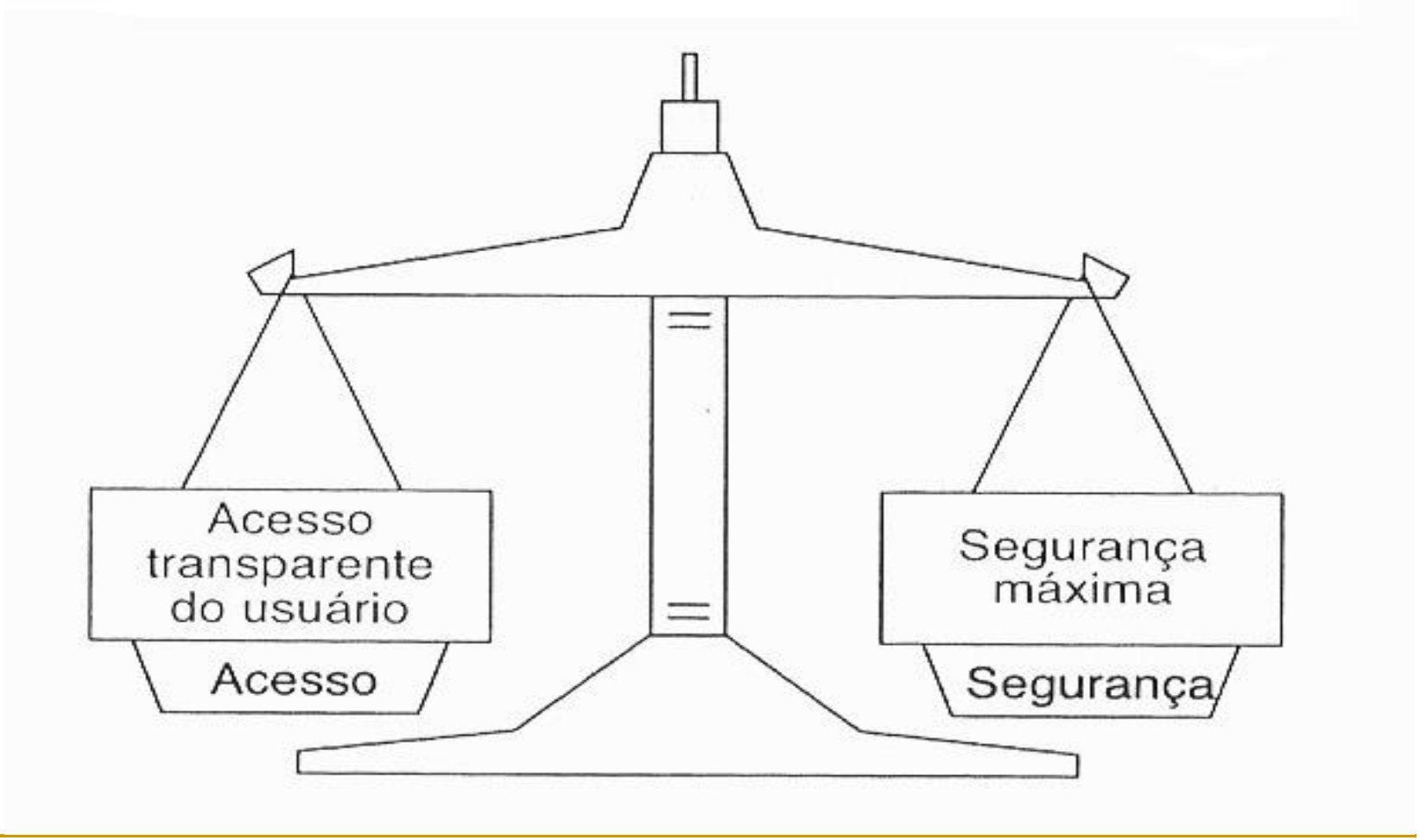


Estudo de Caso 1 - Autenticação e Controle de Acesso

- **Autenticação**
  - PAP (clientes remotos e filiais)

- **Controle de Acesso**
  - listas de acesso em roteadores (WAN e gateway).
  - nenhum firewall
  - nenhuma criptografia

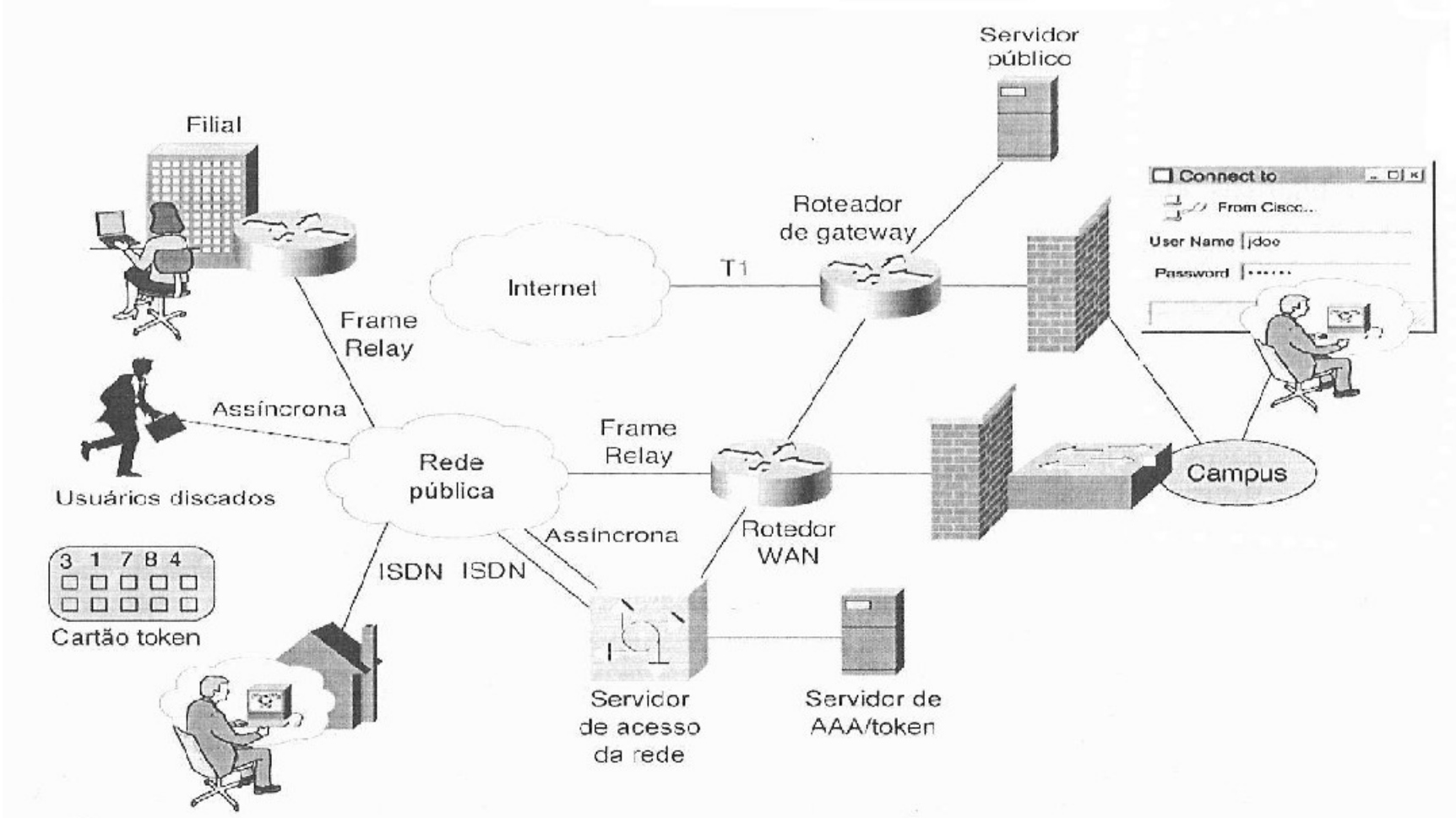
Estudo de Caso 2 – Política de Segurança Restritiva



Estudo de Caso 2 – Política de Segurança Restritiva

- Mais difícil de configurar e administrar.
- Mais difícil para usuários da rede.
- Custo da segurança:
  - US$ 250,00 por computador.

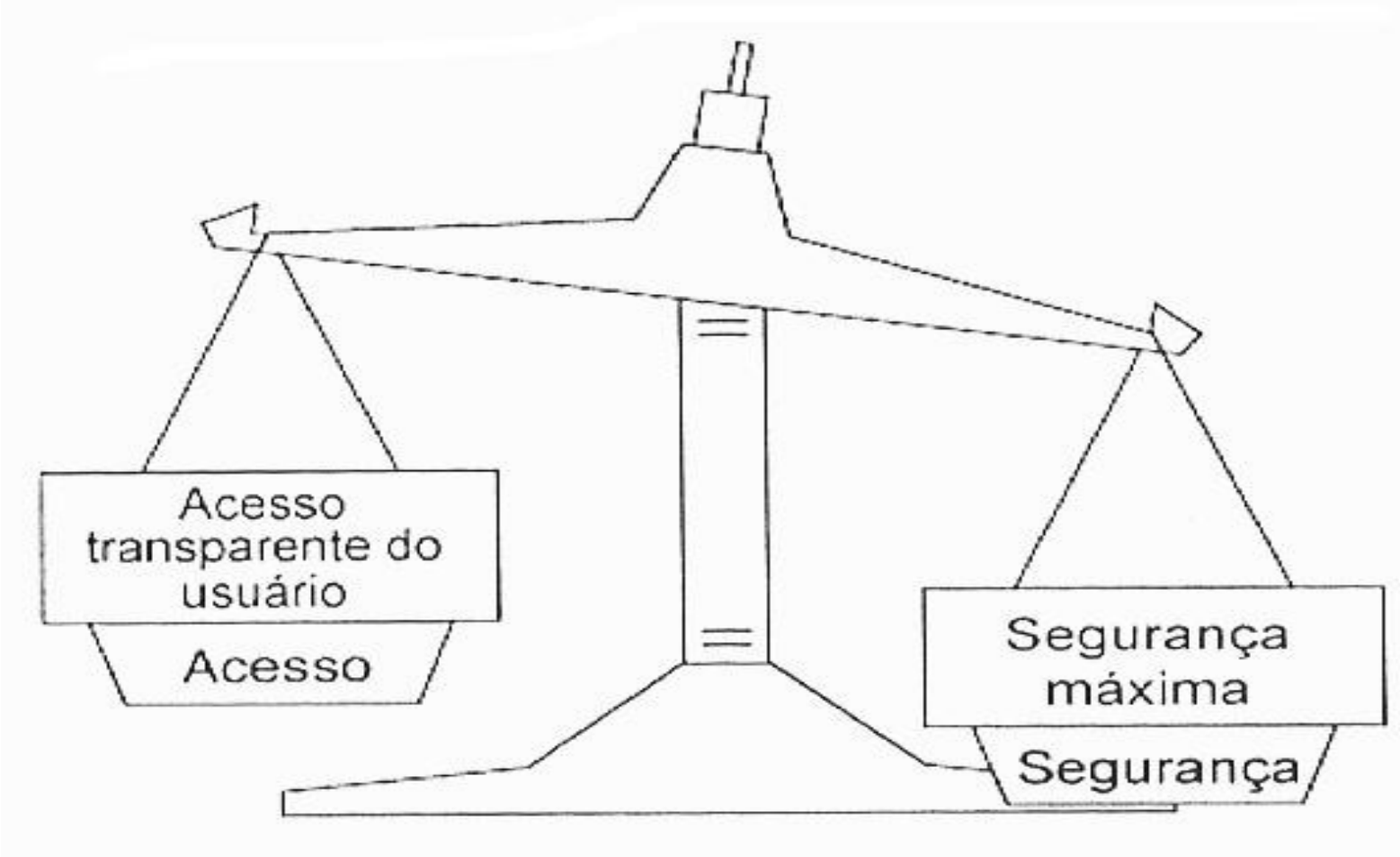
Estudo de Caso 2 – Ambiente de rede para Segurança Restritiva



Estudo de Caso 2 - Autenticação e Controle de Acesso

- **Autenticação**
  - Senhas (discagem, Internet, campus)
- **Controle de Acesso**
  - Listas de acesso em roteadores (WAN e gateway).
  - Firewall entre a Internet e a empresa.
  - Autenticação de rota (filiais e campus)
  - Criptografia (enlaces de filiais)

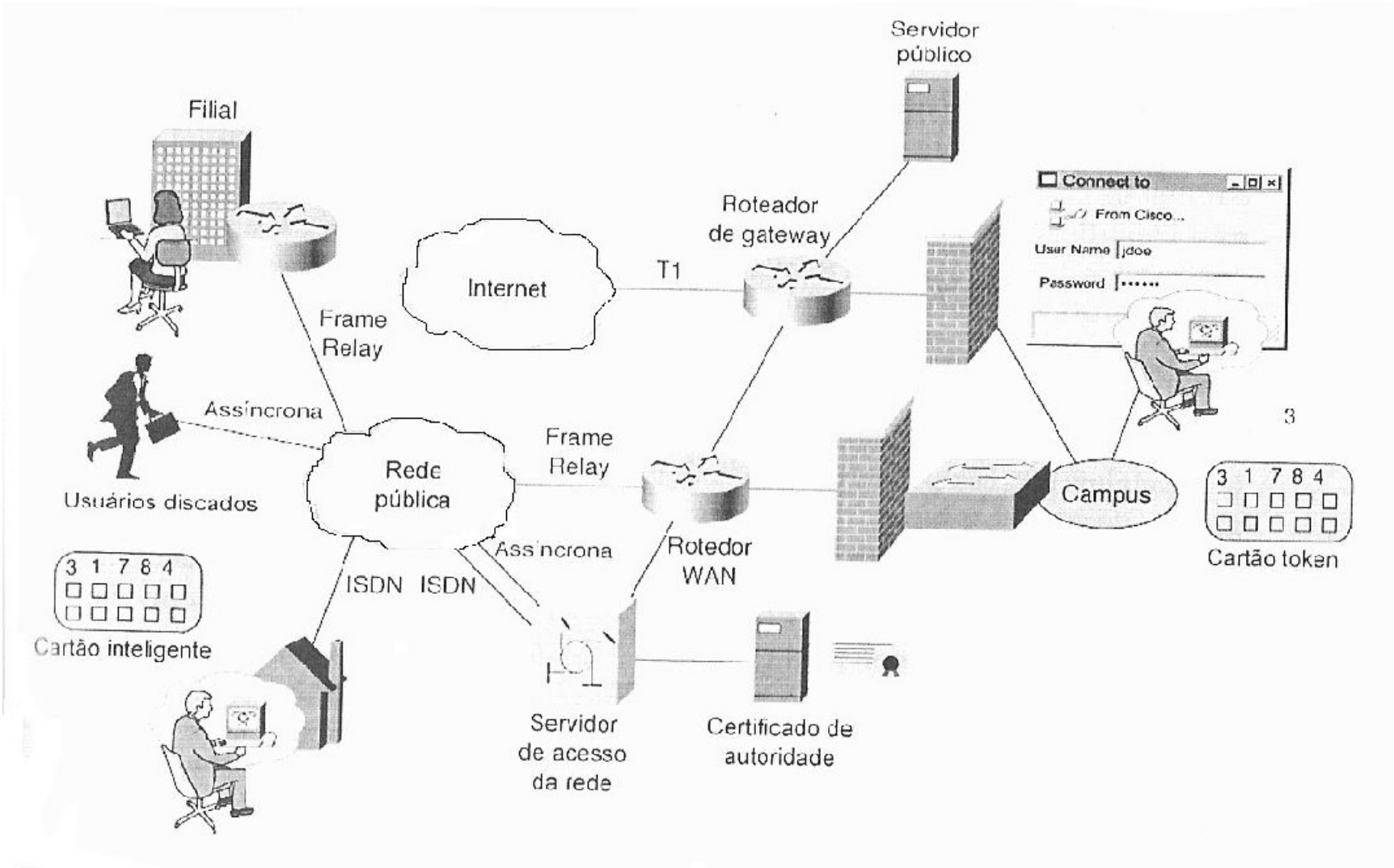
Estudo de Caso 3 – Política de Segurança Fechada



Estudo de Caso 3 – Política de Segurança Fechada

- Mais difícil de configurar e administrar.
- Mais difícil para usuários da rede.
- Custo da segurança:
  - US$ 350,00 por computador

Estudo de Caso 3 – Segurança Fechada



Estudo de Caso 3 – Avaliando a Política de Segurança

- Uma **política de segurança fechada.**
- Conectividade restrita do usuário.
- Menos desempenho.

Política de Segurança Fechada

- Proíbe todas as conexões de rede que não são explicitamente permitidas.
- Define privilégios específicos do usuário.
- Segurança pesa mais do que acesso.

Política de Segurança Fechada

- Mais difícil para os usuários da rede.
- Possuem rede de maior porte.
- Empresas do mercado de serviços financeiros.

Estudo de Caso 3 - Autenticação e Controle de Acesso

- **Autenticação**
  - certificados digitais (linha telefônica, filial e campus).
- **Controle de Acesso**
  - listas de acesso em roteadores: WAN e gateway.
  - Firewall entre a Internet e a empresa.
  - autenticação de rota.
  - criptografia (filiais e campus)

Resumo das tecnologias usadas por empresas, classificadas pelo tipo de política de segurança

Critérios	Aberta?	Restritiva?	Fechada?
Senhas	Sim	Sim	Sim
Cartões de identificação	Não	Não	Sim
Firewalls	Não	Sim	Sim
Criptografia	Não	Às vezes	Sim
Autoridade de certificação	Não	Não	Sim

Resumo dos Estudos de Caso

- A segurança de rede não utiliza um método uniforme.
- A solução para cada empresa é diferente da solução para qualquer outra.
- E poderá ser diferente para uma determinada empresa ao longo do tempo.
- A análise cuidadosa, o planejamento e o uso de ferramentas permitirão aplicar a solução correta, e mais econômica possível.

Política de Segurança da Empresa XYZ

- Ver Cenário de uma Empresa XYZ
- Exemplo completo da política de segurança para a Empresa XYZ.