Tópicos

- Introdução a Segurança
- Os riscos da falta de segurança em sistemas
- Políticas de segurança
- Software de segurança
- Hardware de segurança
- Sistemas de detecção de intrusões (IDS)
- Criptografia e Public Key Infrastructure (PKI)
- Rede privada virtual (VPN)

unic

Introdução a Segurança

- **Não existe sistema 100% seguro!!!**
- História da segurança
  - anos 80 evolução das interconexões de redes
  - aumento da extensão das redes
- O ambiente doméstico
  - Banda larga
  - Internet Banking
- O ambiente corporativo
  - Transações entre corporações
  - Sigilo das informações

unic

Introdução a Segurança

- A necessidade de segurança
  - proteção do patrimônio (no caso a informação)
  - credibilidade e vantagem competitiva
  - cumprimento das responsabilidades
  - continuidade das operações e atividades
- A segurança relativa
  - custo da segurança X valor da informação
  - custo da segurança X tempo da informação
- Análise de risco
  - identificar os “furos” de segurança do sistema
  - determinação da necessidade de segurança

unic

Os riscos da falta de segurança em sistemas

- Os vírus
  - destrutivos
  - de alteração de conteúdo
  - Stephen Hawking – " Primeira forma de vida criada pelo homem"
- Os ataques (Hackers)
  - Cavalos de tróia
  - Sniffer
  - Servidores e serviços mal administrados (Port Scan)
  - Roubo de identidade (Spoof)
  - Quebra de senhas (Password cracking)
  - Engenharia pessoal (convencer alguém de revelar informações)

unic

Políticas de Segurança

- Senhas
  - senhas fortes X senhas fracas
  - não divulgação
  - ser encriptada (função do administrador)
- Administração de pessoal
  - pior das variáveis (citar o casos)
  - instruir os usuários de como operar o sistema
  - instruir os usuários da política de segurança da empresa
  - instruir os usuários do tipo de uso do sistema
  - conteúdos de e-mail
  - SPAM

unic

Políticas de Segurança

- Segurança física de sistemas
  - fator negligenciado por parte dos administradores
  - impedir o roubo de equipamentos
  - acesso físico restrito ao sistema
  - backup das informações (fazer parte da política da empresa)
  - no backup levar em conta os desastre físicos
- Tipo de sistemas de segurança
  - via Software (fraca)
  - via Hardware (forte)
  - combinação Software + Hardware (melhor)
  - todos configurados pelo administrador da rede

unic

Software de Segurança

- Firewall
  - é um sistema de proteção contra acessos não autorizados
  - acesso interno, externo ou ambos
- Softwares
  - Zone Alarm
  - Norton Internet Security
- Bom para usuários domésticos e pequenas empresas
- Não muito eficientes para grandes empresas
- Configuração simplificada
- Anti-vírus ativos

unic

Software de Segurança

- Sistemas Open Source (GNU Linux / Free BSD)
  - grande eficiência
  - mínimos requisitos de hardware
  - maior controle do que acontece em seu interior
  - grande comunidade de auxilio
  - larga experiência na área de segurança
  - maleabilidade das configurações
- Pontos negativos
  - difícil configuração
  - mão de obra especializada
  - investimento em treinamento

unic

Hardware de Segurança

Firewall

- Muitas opções de configuração
- Todo tráfego entre a rede interna e a externa devem passar por ele
- Somente tráfego autorizado passa pelo Firewall
- Administração do controle de acesso centralizado
- Tipo de controle de um Firewall
  - controle de serviço (tipos de serviços autorizados)
  - controle de sentido (fluxo dos serviços)
  - controle de usuário (controle no nível de acesso do usuário)
  - controle de comportamento (como o serviço deve ser usado)

unic

Hardware de Segurança

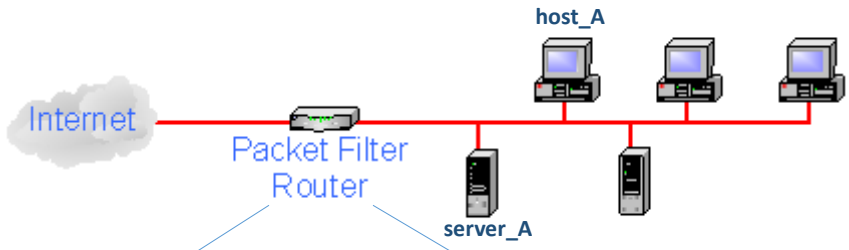
Firewall

- Tipos de firewall
  - filtragem de pacotes
  - gateways de aplicação
  - gateways de circuito
- Estação Bastião
  - máquina segura instalada em um ponto crítico da rede
  - executa SO confiável e estável
  - pode atuar como proxy de serviços Internet
  - pode ser usado para interconectar duas redes (sub-redes)

unic

Hardware de Segurança

Firewall-Filtragem de Pacotes

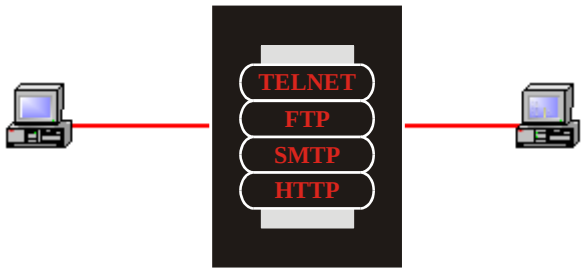


ação	local host	port	remote host	port
allow	server_A	25	*	25
block	host_A	80	*	*

unic

Hardware de Segurança

Firewall-Gateways de Aplicação

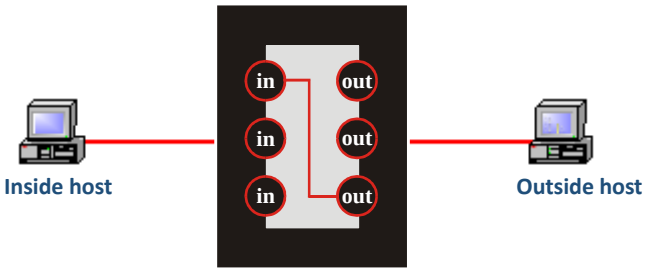


Gateway de aplicação – recebe e transmite uma conexão

unic

Hardware de Segurança

Firewall-Gateways de Circuito

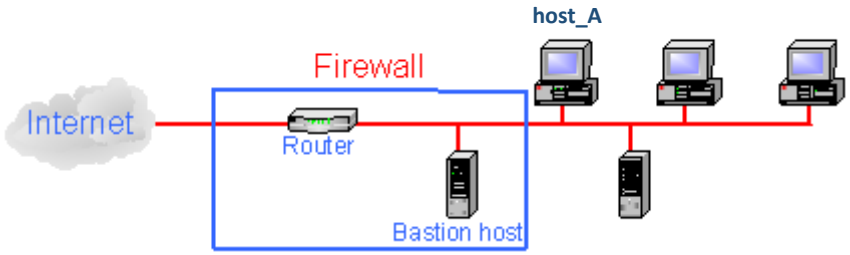


Gateway de circuito – utilização de diferentes portas

unic

Hardware de Segurança

Firewall-Estação Bastião (proxy)

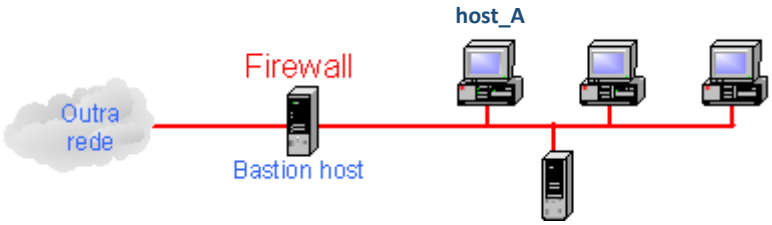


Todas as conexões, entre as rede, devem ser "autorizadas" pelo Bastion host

unic

Hardware de Segurança

Firewall-Estação Bastião (interconexão de redes)



Todas as conexões, entre as rede, passam pelo Bastion host que analisa a possibilidade da conexão

unic

Sistemas de detecção de intrusão (IDS)

- Solução complementar ao firewall
- Software capazes de detectar atividades suspeitas
- Utiliza-se de padrões conhecidos de comportamento de intrusos
- Podem analisar o tráfego interno, externo e entre eles
- Tipos de análise de tráfego
  - Signature detection
  - Behaviour detection
  - Protocol anomaly detection

unic

Sistemas de detecção de intrusão (IDS)

- Signature detection
  - procura de padrões específicos
  - desvantagem - ter de conhecer de antemão o padrão
- Behaviour detection
  - cada rede tem determinada característica (estatística)
  - procura alterações nestas característica (pico de uso fora de hora)
  - desvantagem - método não muito eficaz
- Protocol anomaly detection
  - análise do pacote com seu padrão
  - exemplo: os ataques do Code Red alteram o formato do pacote durante os pedidos HTTP, o IDS detecta esta alteração

unic

Criptografia

- Criptografia – ciência de codificar informações
- Existe há centenas de anos (primeiros indícios – Egípcios)
- Vinha sendo usada no âmbito militar e diplomático
- Nos últimos anos houve um grande avanço na criptografia computacional
- É usada para
  - garantir sigilo (somente usuário autorizados)
  - integridade da informação (não alteração da informação)
  - autenticação dos participantes (confirmação de identidade)
- Para cifrar ou decifrar dados é necessário uma chave ou senha
- Chave – algoritmo matemático de difícil determinação
- Senha – secreta e de difícil determinação

unic

Criptografia

- Tipos de criptografia
  - simétrica (mesma chave/senha para cifrar e decifrar)
  - assimétrica (chaves/senhas diferentes para cifrar e decifrar)
- Criptografia simétrica
  - como passar a senha/chave para o destinatário de forma segura ?
  - eficiente em processos temporários de conexão
- Criptografia assimétrica
  - chave privada (somente o proprietário a conhece)
  - chave pública (todos podem a conhecer)
  - teve maior aceitação devido a sua forma de utilização
  - quando mais divulgarmos a chave pública melhor

unic

Public Key Infraestructure (PKI)

- surgiu da necessidade de gerenciamento de diversas chave públicas
- consiste de serviços, protocolos e aplicações utilizados para o gerenciamento de chaves públicas e certificados
- utiliza de certificados para determinar a autenticidade da chave
- CA (Certification Authority) entidade de confiança que deterá em seu poder as chaves públicas de diversos usuários
- centralização das chaves publicas dos usuários
- os benefícios de uma solução PKI
  - autenticação
  - confidencialidade
  - integridade
  - controle de acesso
  - privacidade
  - não-repúdio

unic

Assinatura Digital

- versão digital da assinatura de uma pessoal
- destinatário pode comprovar a assinatura digital, dando assim credibilidade a informação transmitida
- quando verificada uma assinatura digital não pode ser negada (não repudio)
- garantem a integridade do documento
- garantem a legitimidade do remetente
- exemplo, para personalizar uma mensagem, um determinado usuário **'A'** codifica uma mensagem utilizando sua chave secreta e a envia para o destinatário. Somente a chave pública de **'A'** permitirá a decodificação dessa mensagem. Portanto é a prova de que **'A'** enviou a mensagem
- a mensagem pode ser decodificada por qualquer um que tenha a chave pública do remetente

unic

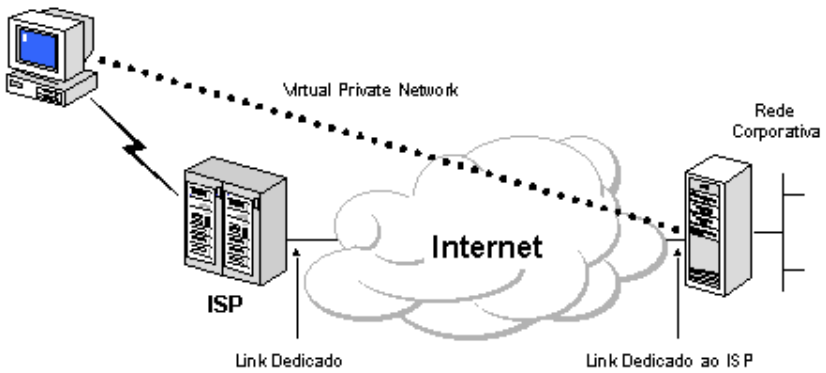
Rede Virtual Privada (VPN)

- Provem segurança através de redes inseguras (ex. Internet)
- Nível de segurança aceitável
- Bom para administração remota
- Redução de custo de links
- Pode ser implementada através de links dedicados ou não
- Ponto negativo: desempenho e/ou atraso
- Aplicações
  - acesso remota via Internet
  - interconexão de redes via Internet
  - interconexão dentro de uma rede (restringir acessos)

unic

Rede Virtual Privada (VPN)

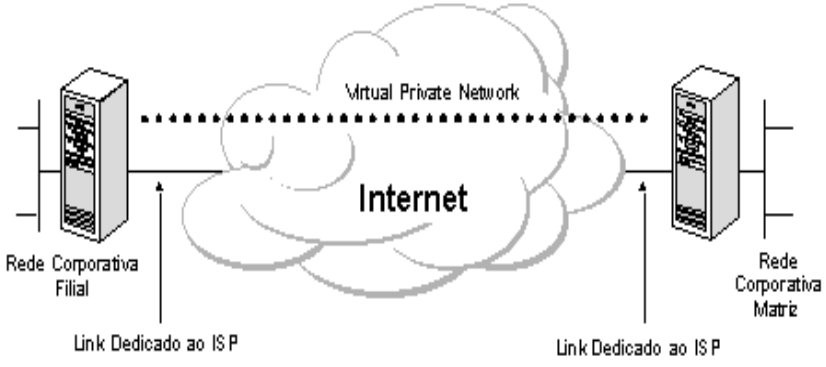
Acesso remoto via internet



unic

Rede Virtual Privada (VPN)

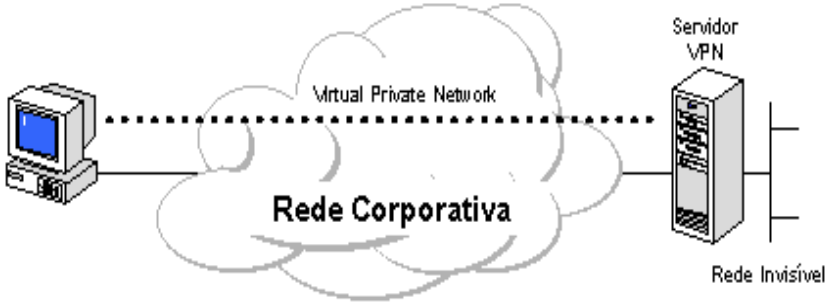
Interconexão de redes via internet



unic

Rede Virtual Privada (VPN)

Interconexão dentro de uma rede via intranet



unic

Conclusão

- Crescente necessidade de segurança (doméstico e corporativo)
- Área em expansão (falta de bons profissionais)
- Administradores competentes (administrar o sistema e o pessoal)
- Não existe sistema 100% seguro, o que existe é um sistema mal configurado

- Dúvidas?
- Perguntas?

unic