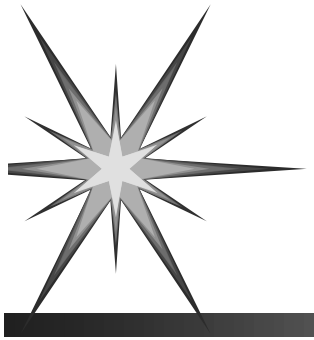
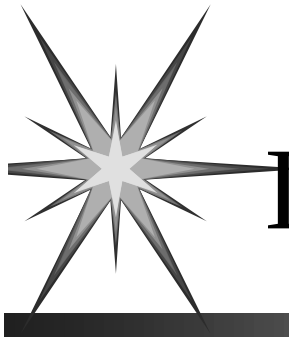


Segurança de Sistemas e Internet Firewalls

Marcos Aguinaldo Forquesato
Centro de Computação
UNICAMP

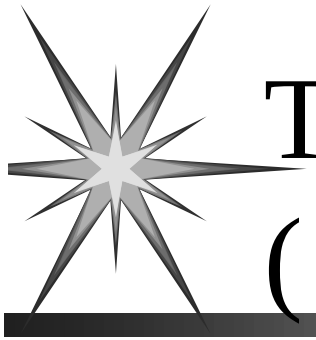
Por que você precisa de segurança?

- Para proteger sua rede contra a invasão de pessoas não autorizadas
  - INTERNET (NW - Julho/98)
    - ~ 36.739.000 computadores
    - ~ 13.062.628 domínios (nível 3)
    - ???.???.??? usuários -> 150.000.000 (1 %)
  - INTERNET Brasil (CG)
    - ~ 163.890 computadores
    - ~ 23.941 domínios
    - ~ 1.310.001 usuários - Dezembro/97 (1 %)



Incidentes nos USA (CERT) :

- 1992 773
- 1994 2.340
- 1996 2.573
- 1997 2.134 (> 100.000)
- 1-3Q 1998 2.497
- 4 % detectam as tentativas de invasão
- 40 % dos ataques obtém permissão de super-usuário



Teste do Departamento de Defesa (USA - 1995)

- 8.932 sistemas participantes
- 7.860 foram invadidos com sucesso
- 390 detectaram os ataques
- apenas 19 relataram os ataques

O que você está tentando proteger?

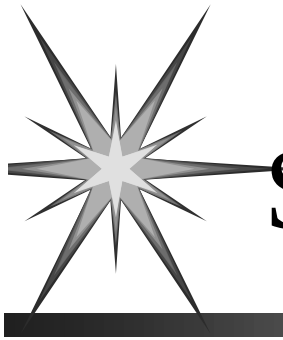
- Seus dados
  - Integridade
  - Privacidade
  - Disponibilidade
- Seus recursos
- Sua reputação

Riscos na Internet

- Estelionato / Sedução / Conto do Vigário
- Perda da Performance
- Violação de direitos autorais
- Repúdio de informações
- Falsos Sites/Identidades
- Fraudes
- Violação de correspondência

Contra o que você está tentando se proteger?

- Classes de Ataques
  - Roubo de senhas
  - Engenharia Social
  - BUG & Backdoors
  - Falha de autenticação
  - Falha de protocolo
  - Obtendo Informações
  - Negando serviços



Segurança das Contas

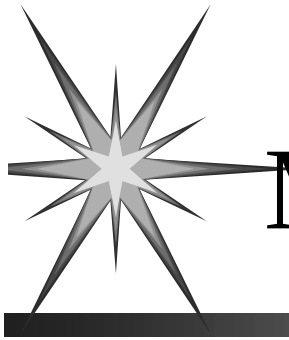
- Senhas
  - Seleção adequada
  - Políticas para escolha
  - Verificação periódica da segurança (Crack)
  - Datas de expiração
- Contas guest
- Contas sem senha
- Contas de grupo -> Mecanismo de grupos

Segurança do Sistema de Arquivos

- Verificação periódica dos arquivos com suid/sgid
- Remova os suids desnecessários dos filesystems (locais e remotos)
- ACLs
- Nunca utilize shell scripts com o suid bit
- umask (027 ou 077)
- Dispositivos

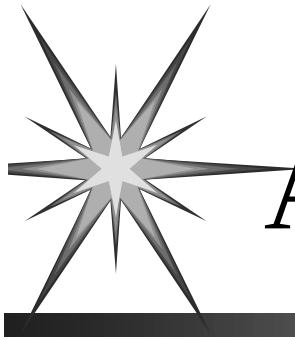
Segurança do Sistema de Arquivos

- Arquivos imutáveis
- Montar filesystems read-only
- Network File System (NFS)
  - /etc/exports (-access)
  - Restrição de acesso para o root
  - nosuid/nodev
- BACKUPs



Monitoração da Segurança

- Checklists diários
  - /etc/passwd (formato/conteúdo)
  - arquivos suid/sgid
  - arquivos sem dono
  - .rhosts
- Tripwire
- COPS/Tiger

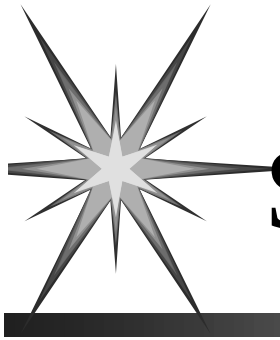


Auditoria

- Log Host
- lastlog
- utmp
- wtmp
- acct

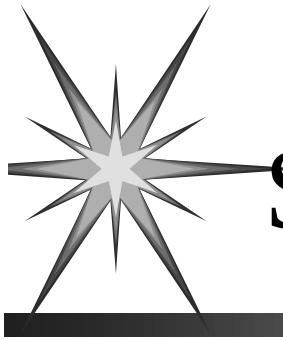
Auditoria

- syslog
- messages
- sulog
- xferlog



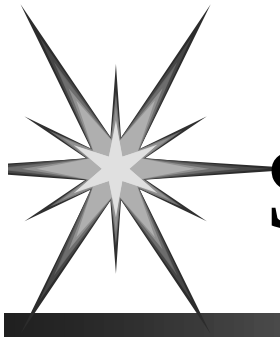
Segurança Física

- Backups
- Plano de contingência
- autologout
- xautolock



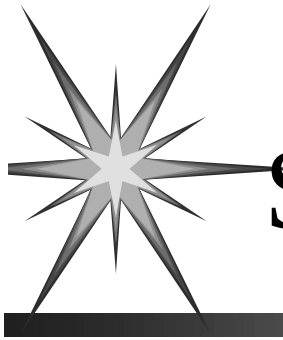
Serviços

- "r" commands -> SSH
- /etc/hosts.equiv - $HOME/.rhosts
- lpd -> LPRng
- NIS
- NFS -> DFS
- /etc/hosts.lpd
- fingerd



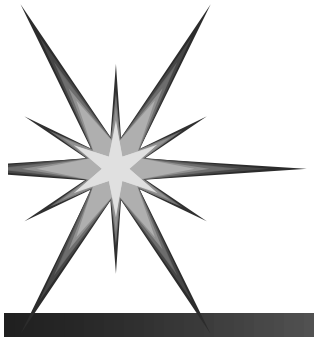
Serviços

- DNS (zone transfer)
- Trivial ftp (tftp)
- NNTP/INND
- POP/IMAP
- /etc/aliases
- Sendmail (smrsh - procmail)
- majordomo/petidomo

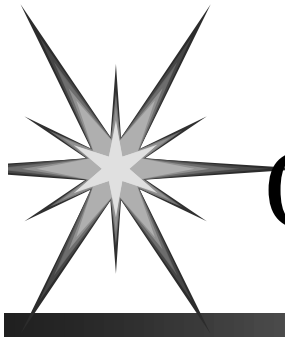


Serviços

- Terminais seguros
- UUCP
- World Wide Web (WWW)
  - Rode o httpd com o usuário nobody
  - CGI scripts
  - Monitore as logs (access.log)
- anonymous ftp

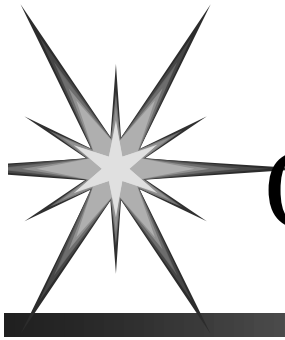


Internet Firewalls



O que é um Internet Firewall?

- Restringe acessos a um local cuidadosamente controlado
- Impede que invasores alcançem suas demais defesas
- Restringe saídas de um local cuidadosamente controlado

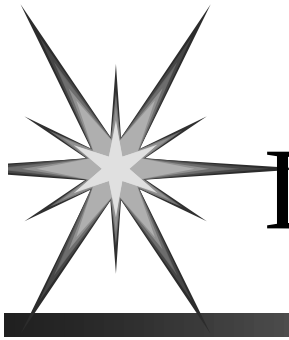


O que um Firewall pode fazer?

- Forçar a política de segurança
- Logar todo tráfego
- Limitar riscos
- Um firewall é um foco de decisões

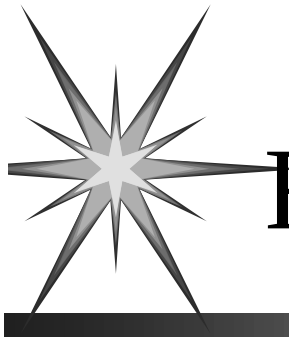
O que um Firewall não pode fazer?

- Proteger contra pessoas internas
- Proteger contra conexões que não passam por ele
- Proteger completamente contra novos caminhos



Definições

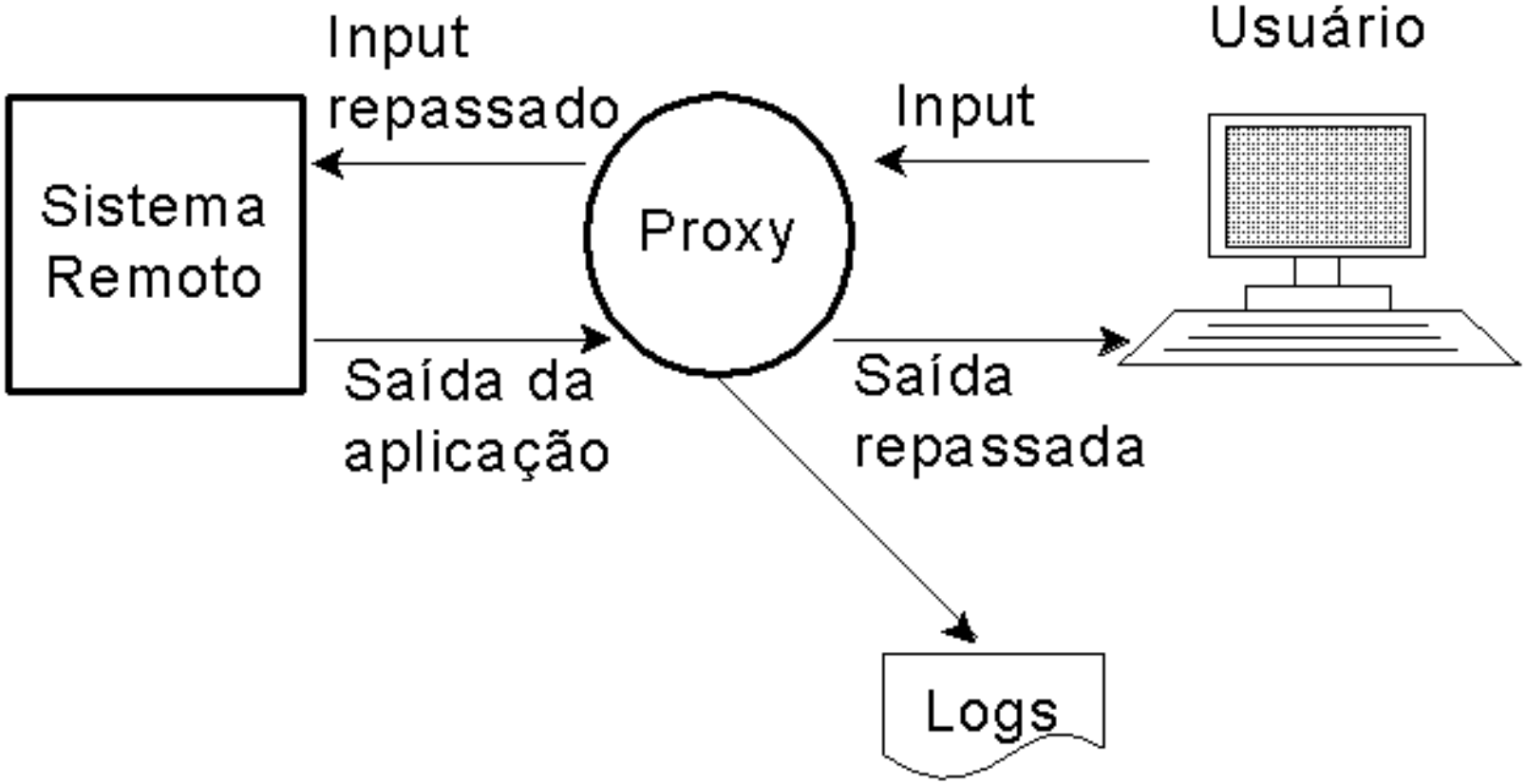
- Filtros de pacotes
- Proxy / Aplicação Gateway

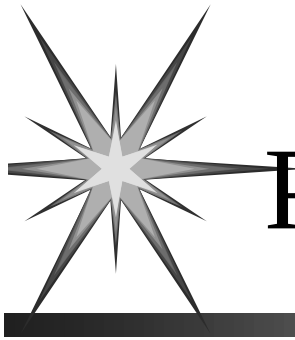


Filtros de pacotes

- Controle de acesso
  - Endereço de origem e destino
  - Protocolo (TCP, UDP ou ICMP)
  - Porta de origem e destino (TCP ou UDP)
  - Tipo de mensagem ICMP
  - Interface de rede de entrada e saida
  - TCP flags
  - Fragmentos

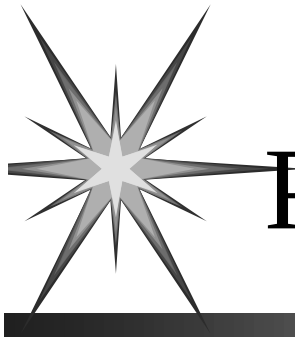
Proxy / Aplicação Gateway





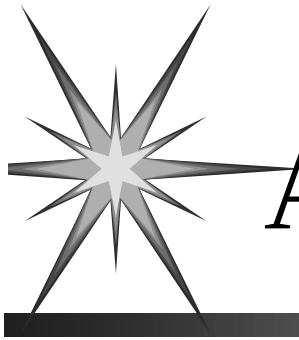
Proxy / Aplicação Gateway

- Recebe as conexões e repassa a entrada de dados (input) para o sistema remoto. A aplicação responde aos proxies que repassam a saída (output) para o usuário.
- Controle de acesso
- Verifica o protocolo de cada aplicação
- Loga o tráfego
- Pode possuir mecanismos anti-virus



Proxy / Aplicação Gateway

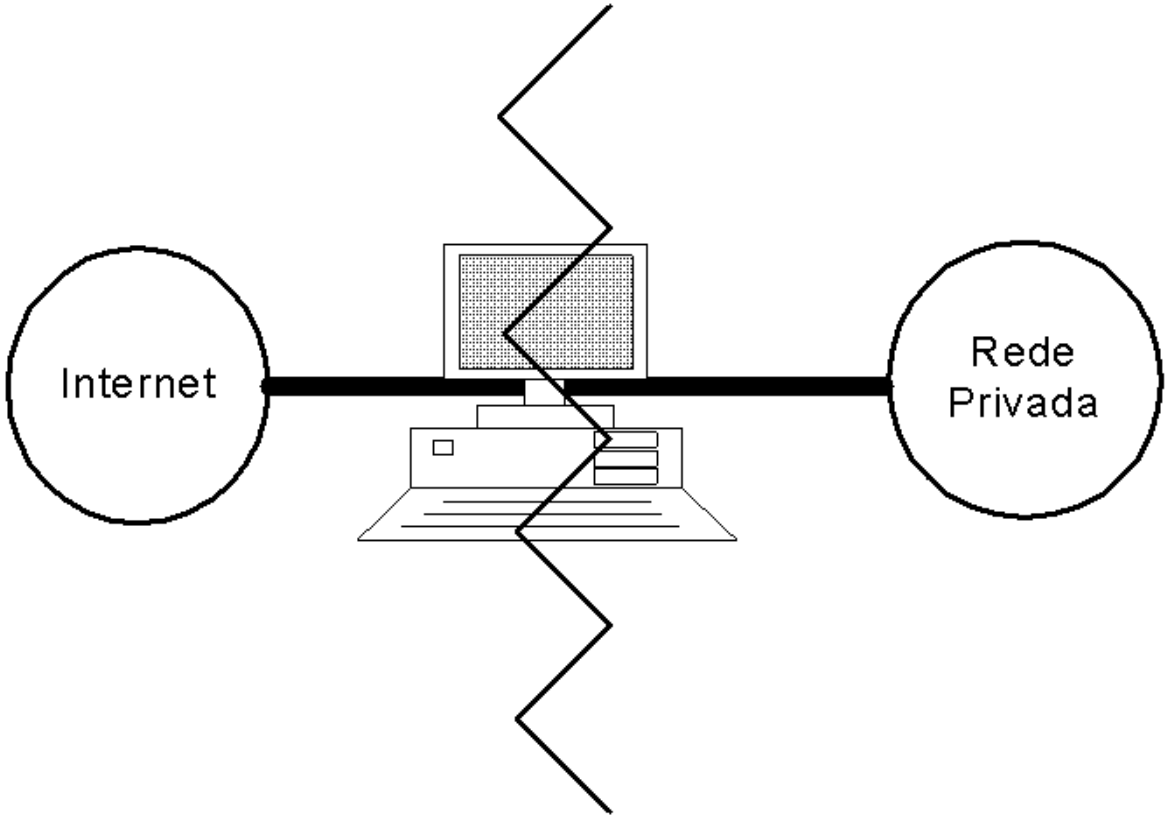
- Exemplos :
  - Sendmail (smapd - smtpd/smtpfwdd)
  - Telnet gateway
  - FTP gateway
  - X11 protocol forwarder
  - HTTP gateway (Screening)



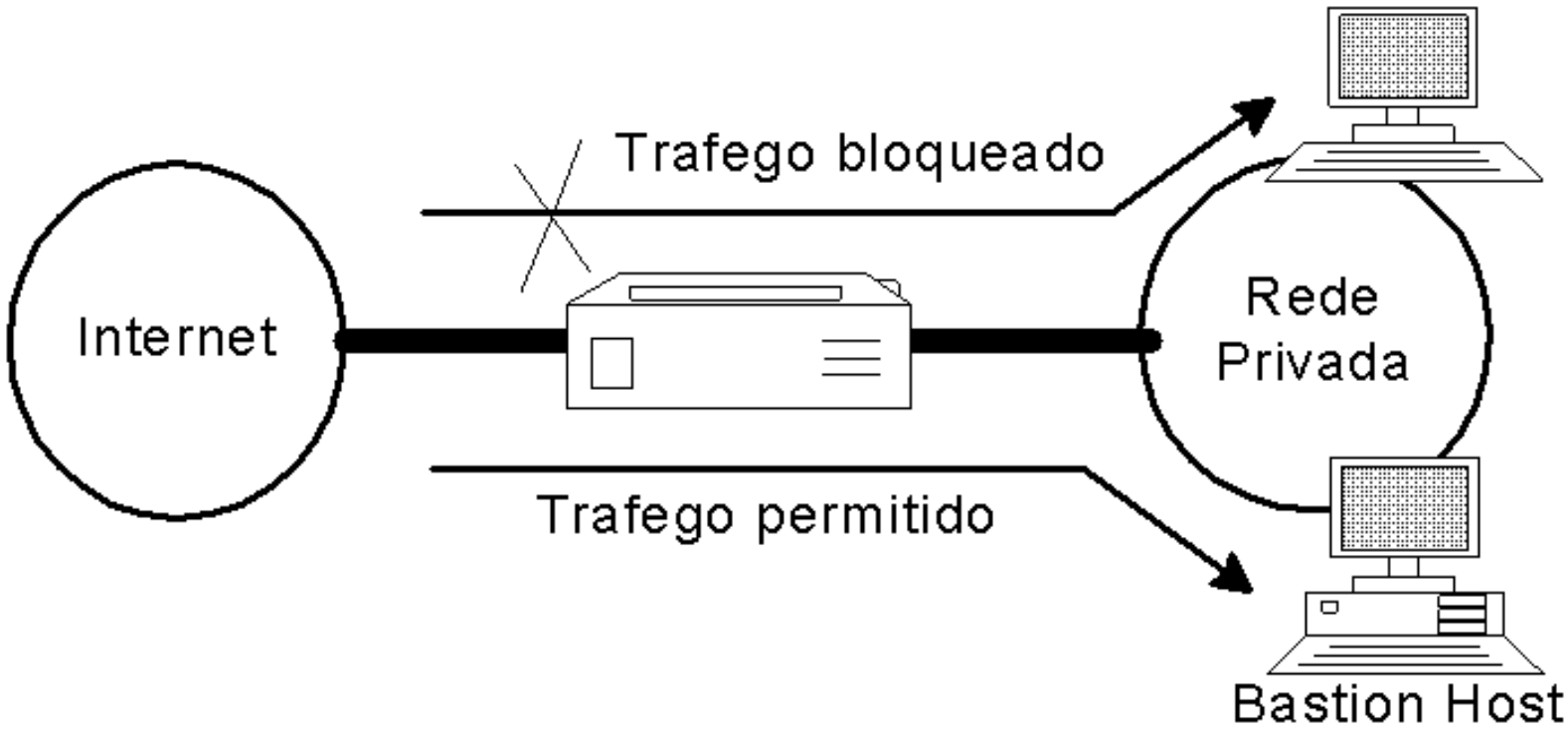
Arquiteturas de Firewall

- Dual-Homed Host
- Screened Host
  - Bastion Host
- Screened Subnet
  - Rede perimetral (Zona desmilitarizada)
  - Bastion Host
  - Roteador interno
  - Roteador externo

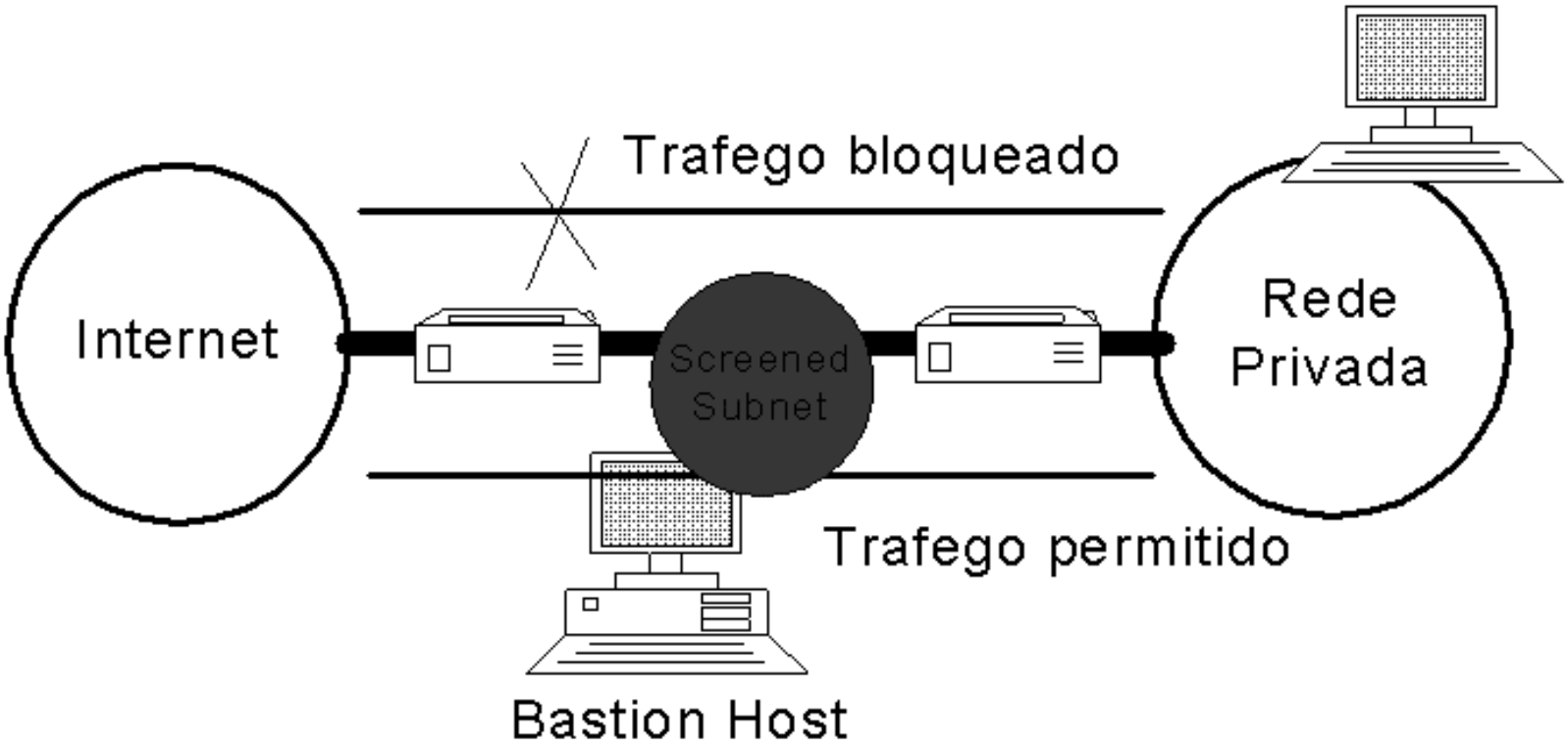
Dual-Homed Gateway

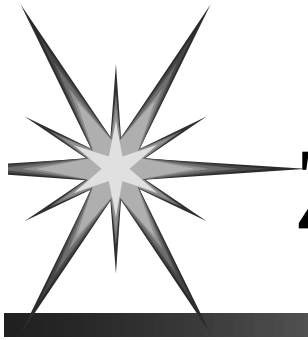


Screened Host



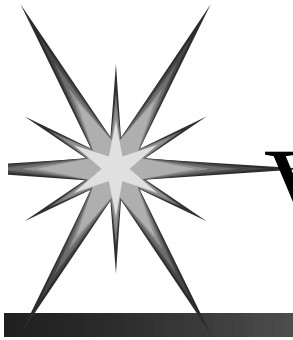
Screened Subnet





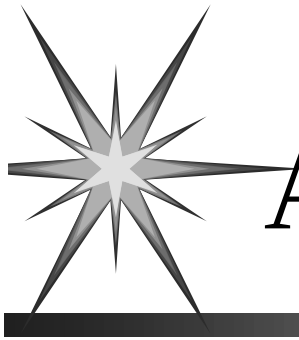
Zona desmilitarizada (DMZ)

- Subrede localizada entre a rede externa (Internet) e a rede interna (rede privada)
- Pode ser a terceira interface de um gateway



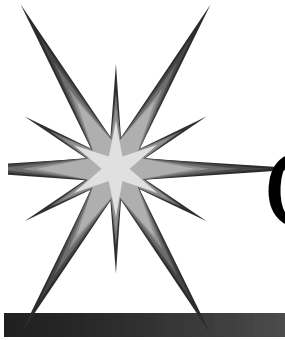
Variações sobre as arquiteturas

- Múltiplos bastion hosts
- Juntar o roteador externo e interno
- Múltiplos roteadores externos
- Múltiplas redes perimetrais
- Usar Dual-Homed Hosts e Screened Subnet



Autenticação

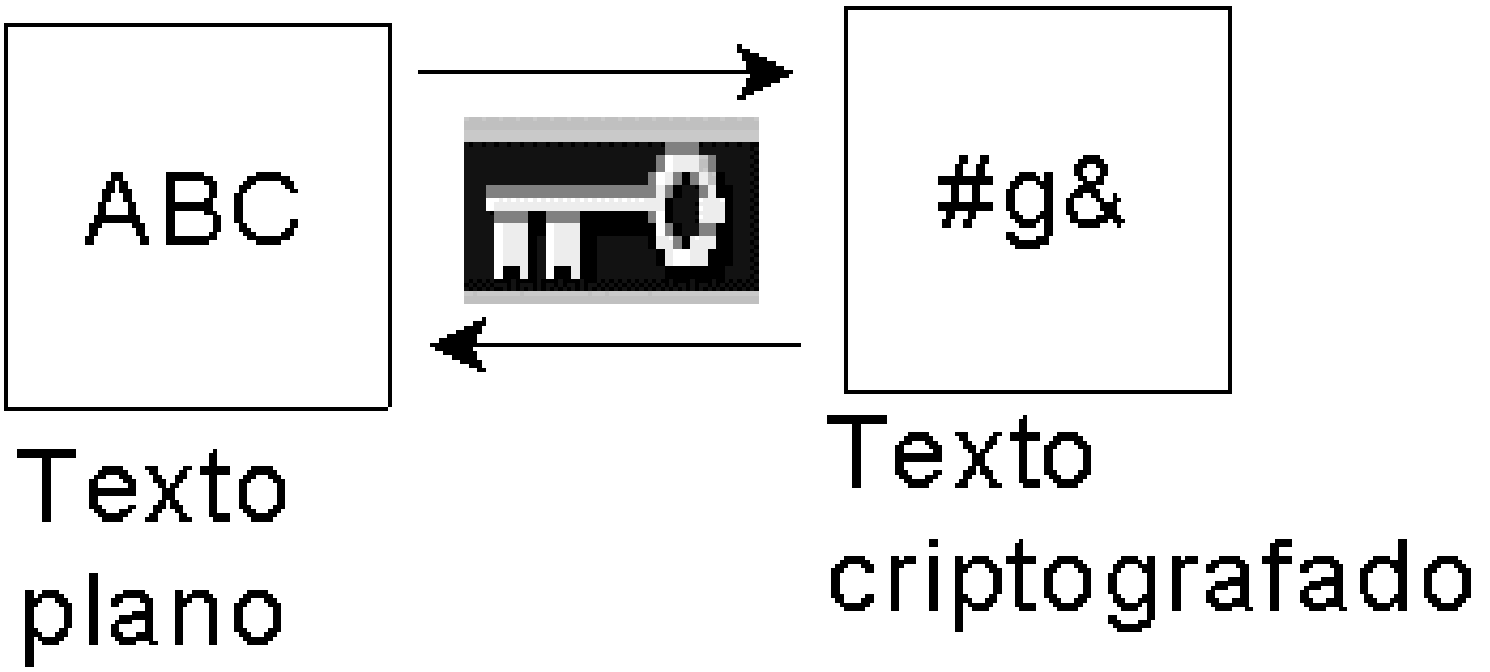
- One-time passwords
  - Programa/Calculadora
  - Lista de senhas
  - Ex: S/Key (jotp) - OPIE
- Smart Card
  - Ex: SecurID



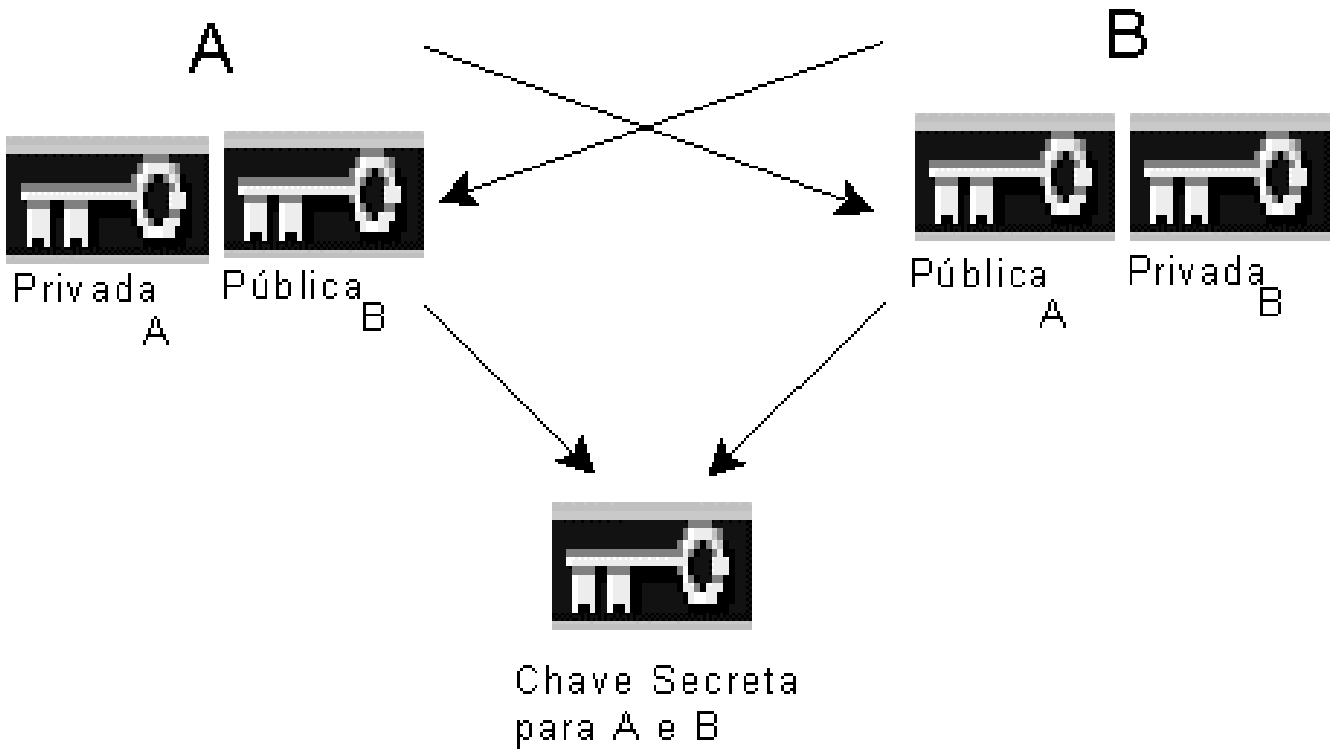
Criptografia

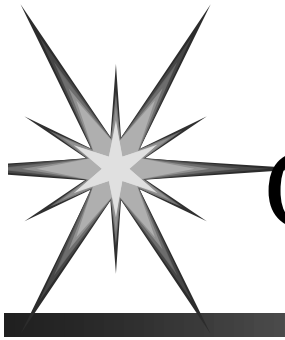
- Simétrica
- Assimétrica

Criptografia Simétrica



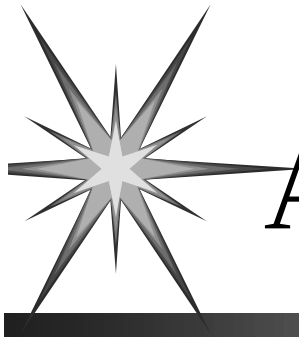
Criptografia Assimétrica





Certificação

- Verifica a chave pública
- Necessita de um terceiro elemento , conhecido como Autoridade Certificadora (CA)

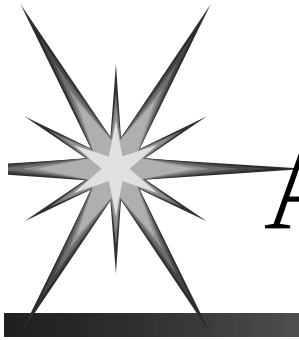


Assinatura Digital

- Certificados são conhecidos como assinaturas digitais
- A chave pública pode verificar a integridade de um documento através da assinatura digital

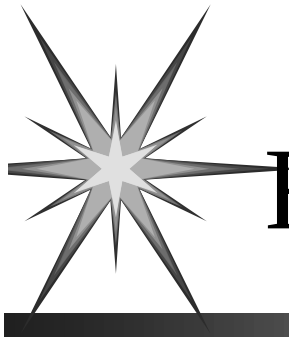
Network Address Translation (NAT)

- Mecanismo que troca o endereço IP de máquinas da rede interna para o endereço do firewall (ou um range de endereços)
- Os IPs internos não são de conhecimento público



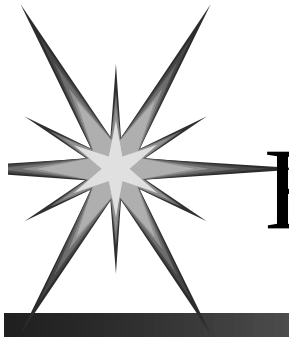
Administração do Firewall

- Alertas
- Auditoria
- Atendimento a emergências de segurança



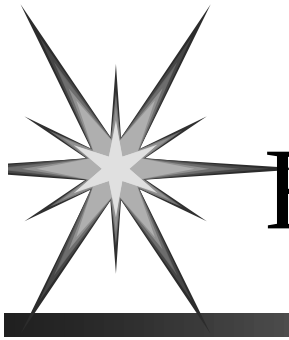
Ferramentas

- Ferramentas de autenticação
- Ferramentas de análise
- Filtros de pacotes
- Sistemas proxies
- Ferramentas de criptografia
- Daemons
- Utilitários
- Produtos comercias



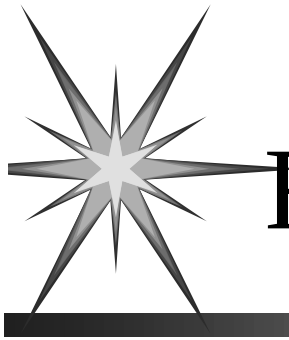
Ferramentas de autenticação

- TIS Internet Firewall Toolkit
- Kerberos
- DCE



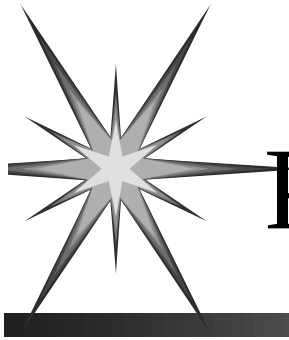
Ferramentas de análise

- COPS / Tiger
- Tripwire
- SATAN (Security Administrator Tool for Analyzing Networks)
- ISS (Internet Security Scanner)
- Strobe
- Nessus



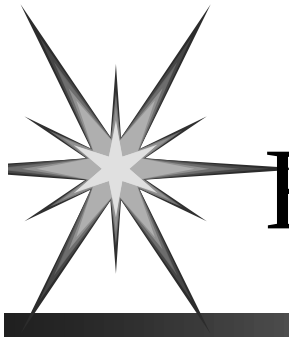
Filtros de pacotes

- IPfilter
- IPFW



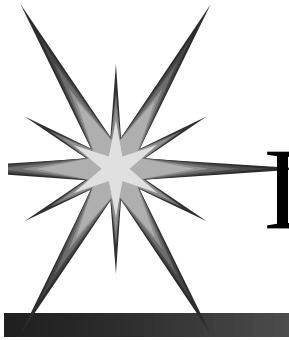
Proxies

- SOCKS
- TIS Internet Firewall Toolkit
- UDP Packet Relayer
- rinetd
- Bjorb/stunnel



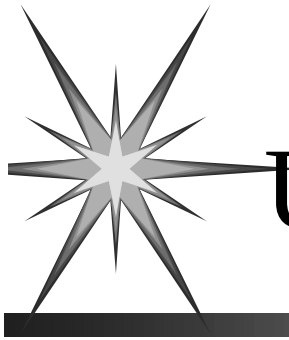
Ferramentas de criptografia

- SSH (Secure Shell)
- SSL (Secure Socket Lawer) - SSLtelnet/SSLftp
- PGP (Pretty Good Privacy) - gnupg



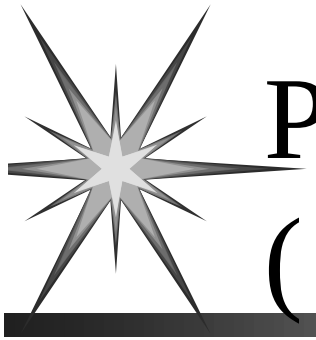
Daemons

- wuarchive ftpd
- gated
- NIS+
- DFS
- xntpd



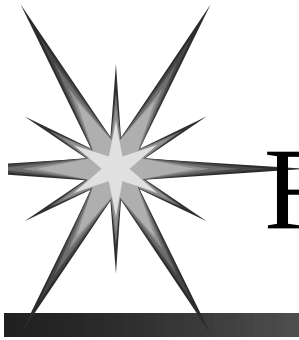
Utilitários

- TCPwrapper
- chrootuid
- swatch/logsurfer
- trimlog
- tcpdump/tcpshow



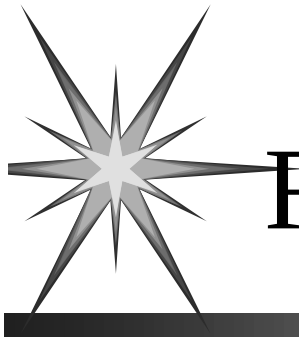
Produtos comercias (38 empresas)

- Firewall-1 (Checkpoint)
- Altavista Firewall
- Gauntlet Firewall (TIS)
- Firewall Aker (brasileiro)



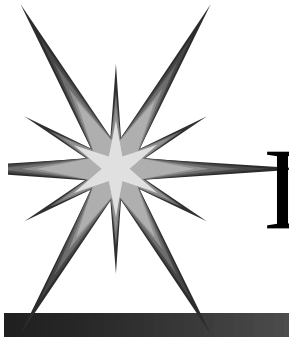
Referências

- Livros :
  - Firewalls and Internet Security
  - Building Internet Firewalls
  - Practical Unix & Internet Security
  - Computer Crime



Referências

- Links :
  - COAST Homepage - www.cs.purdue.edu/coast
  - CERT Coordination Center - www.cert.org
  - NIC-BR - www.nic.br
  - Pangéia - www.pangeia.com.br



Listas

- seguranca@pangeia.com.br
- cert-br@pangeia.com.br
- nbso@nic.br
- BUGTRAQ@NETSPACE.ORG
- firewalls@GreatCircle.COM