

Aspectos a Serem Considerados

Rodrigo Rubira Branco
rodrigo@firewalls.com.br

O que é a Firewalls?

- **Empresa Especializada em Segurança;**
- **Profissionais Certificados;**
- **Atenta a Padrões Internacionais;**
- **Parceira das maiores empresas de Segurança do Mundo;**
- **Visão de Negócios e Ética Empresarial;**
- **Soluções Personalizadas para a Realidade das Empresas;**
- **Independente de Fornecedores e Tecnologias proporcionando a melhor solução para o cliente específico.**

O que a Firewalls tem?

- **Treinamentos em Segurança;**
- **Implementação de Infra-Estrutura de Redes;**
- **Implementação de Análises de Risco e Vulnerabilidades;**
- **Implementação de Detectores de Intrusão e Políticas de Segurança;**
- **Consultoria em E-commerce e Desenvolvimento;**
- **Divisão de Alta Disponibilidade e Disponibilidade Contínua;**
- **Homologação de Firewall.**

SOPHOS anti-virus and anti-spam for business



(nfr)(security)



"If you want steel doors and shutters on your network, NFR is the one for you."

- SC Magazine



NORMAN

3M Worldwide



- **Expor os problemas existentes na escolha de soluções de segurança;**
- **Demonstrar as características de diversas soluções de segurança;**
- **Fornecer dados para escolha das melhores soluções, independentemente de fornecedores.**

**O que não será visto?
“Techniques”**

CIDAL =

Confidencialidade

Integridade

Disponibilidade

Autenticidade

Legalidade

**LEMBRAR-SE SEMPRE DISTO NO DECORRER DA
PALESTRA!**

Trabalhamos em um mundo real de sistemas mal configurados:

- * Bugs de Software**
- * Empregados Insatisfeitos**
- * Administradores de Sistemas Sobrecarregados**
- * Acomodação de necessidades empresariais**
- * Falta de Educação em Segurança**
- * B2B,B2C,B2E,C2C,X2X?**

Defense In-Depth

- **Um Firewall apenas aumenta o nível de segurança;**
- **O conceito de segurança em camadas garante que as falhas existentes em um Firewall sejam supridas por outros tipos de defesa e segurança;**
- **Através de diversas camadas cria-se um modelo de segurança robusto e capaz de suportar falhas.**

Quando pensar em Segurança pense em uma CEBOLA.

- Roteadores;
- Firewall;
- IDS x IPS;
- Análise de Vulnerabilidades x Teste de Intrusão;
- Antivírus/Antispam;
- Gerenciamento/Suporte;
- Normatizações x Políticas;
- Coletores/Analísadores de Logs;
- Fortalecimento de Servidores;
- Forense/Reatividade;
- Capacitação/Treinamentos;
- Firewalls x Concorrentes?

- **Primeiro elemento exposto a Redes não-confiáveis (internet);**
- **Último elemento a defender a rede interna no tráfego que sai.**

- **Recursos de ACL (filtro de pacotes) que podem fortalecer e impor políticas de segurança, aliviando tecnologias de Firewall por ser um processo de filtragem simples (conceito de defense in-depth);**
- **Recursos de QoS e Controle de Banda podem auxiliar contra ataques DoS e uso irregular dos recursos de rede por parte da rede interna;**
- **Segurança/Fortalecimento do próprio roteador evitando invasões (possui um software para roteamento, que utiliza-se de um sistema operacional que pode ser invadido – além dos serviços que executa).**

- **Ferramenta mais conhecida e difundida;**
- **Possui diversas ramificações e tecnologias;**
- **Fornece um ponto de fortalecimento e imposição das políticas empresariais;**
- **Pode ser integrado a outras soluções.**

- **Filtro de Pacotes x Com estado (stateless x stateful);**
- **Integração com outros produtos (antivírus, ids);**
- **Gerenciamento centralizado de múltiplos pontos;**
- **Imposição de políticas de segurança (tudo aquilo que é normatizado mas não é imposto tende a fracassar);**
- **“Permite passar somente aquilo que for expressamente permitido E aquilo que conseguir!”**

- **IDS -> Visa detectar e alertar ataques (pode ser integrado com um Firewall para realizar bloqueios ou também interferir na seção enviando um RST);**
- **IPS -> Faz parte do tráfego de forma in-line, detectando e bloqueando os mesmos;**
- **Falsos Positivos x Falsos Negativos;**
- **Gerenciamento de múltiplos sensores;**
- **Gerenciamento de logs centralizado;**
- **Integração com outras soluções;**
- **OSEC x OPSEC;**
- **Capacidade de análise (gigabit x fast);**
- **Inteligência x Pura comparação;**
- **Por assinaturas x Por padrão.**



- **Análise de Vulnerabilidades -> Não intrusivo, verifica e alerta sobre possíveis falhas em sistemas (estruturais, físicas, técnicas, de configuração);**
- **Teste de Intrusão -> Realização em si de intrusões, alertando falhas que possam ser exploradas, mas não fornecendo maiores informações para prevenção;**
- **Verificação de aplicações (onde nossas Faculdades erram);**
- **Ferramentas Comerciais e a análise automatizada.**

- **MOSTRAR OS CUSTOS QUE ANOTEI NO EVENTO;**
- **Atualizações "reais";**
- **Distribuição de atualizações centralizada;**
- **Produtos corporativos.**

- **Custo de profissional específico em segurança**
- **Custo de um administrador de sistemas que também faz segurança;**
- **Suporte de vários tipos, para várias empresas;**
- **O que buscar?**
 - * **SLA**
 - * **Experiência**
 - * **Profissionais certificados**

- **Muitas normas de segurança da informação existem (BS 7799, NBR/ISO 17799, ISO 14408);**
- **Seguir todas as normas pode vir a atrapalhar o andamento da empresa, ou até mesmo ser inviável;**
- **Políticas internas precisam ser Impostas e não apenas definidas;**
- **Dados devem ser seguidos para estabelecimento de um projeto Real (pegar da apostila de IDS o termo SMART).**

- Para que logs se não forem coletados centralizadamente (ninguém irá por todos os equipamentos da empresa verificá-los)

OBS: Empresas pequenas podem pensar que não têm mais que um servidor (talvez um Firewall para compartilhamento internet), mas no entanto possuem necessariamente:

- Tal equipamento de compartilhamento;
- Roteador (chamem de modem, ou qualquer coisa, mesmo ADSL);
- Equipamento utilizado para os dados administrativos;
- Talvez um servidor do sistema interno (mesmo que este apenas guarde um BD compartilhado);
- Coletar os logs não basta, é necessário analisá-los e o fato de diferentes sistemas possuírem diferentes formatos faz com que aplicações existam para isto.



- **Exige profissional capacitado nas soluções instaladas (Sistema operacional, softwares aplicativos);**
- **Fortificação de configurações;**
- **Fortificação de Sistema Operacional (Linux, Windows, etc);**
- **Configuração de logs (a serem armazenados centralizadamente ou coletados).**

- **Com a Firewalls não seria necessário? Sim, talvez seja;**
- **Reatividade não proatividade? Digamos então, reatividade controlada;**
- **Análise Forense pode ser essencial em caso de uma interpelação judicial (coleta de provas);**
- **Advogados especializados em Informática são difíceis de se encontrar, e profissionais não especializados podem levar a perdas maiores do que o próprio incidente.**

- **Como treinar em segurança, sendo que segurança envolve praticamente TUDO?**
- **Processos;**
- **Pessoas;**
- **Equipamentos/Servidores;**
- **Estações;**
- **Aplicações;**
- **Meio ambiente, natureza, etc;**

- **Treinamentos Técnicos? Administrativos?**
- **Revistas e Livros do "Como ser hacker".**

- **Não concorreremos, formamos parcerias;**
- **Metodologias, padronizações, organização, experiência, conhecimento técnico;**
- **Procure um representante Firewalls em sua região ou contate-nos diretamente.**

FIM! Será mesmo?

DÚVIDAS?!?

Rodrigo Rubira Branco
rodrigo@firewalls.com.br