SEGURANÇA

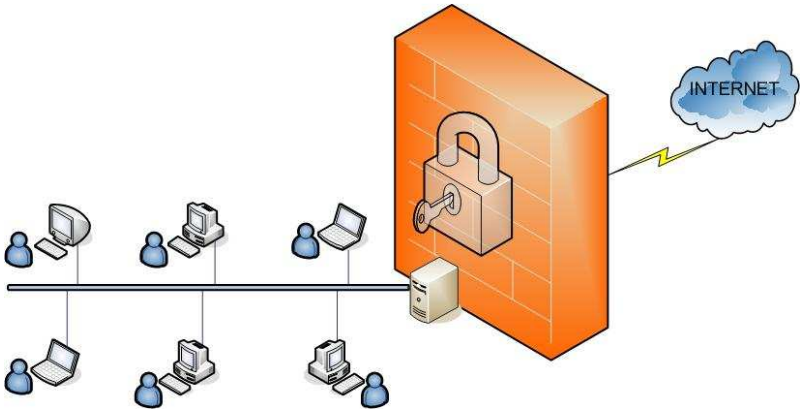
Firewall de Rede

A Compy oferece soluções de segurança extremamente robustas, que apresentam baixo custo com altíssima confiabilidade.

"Antigamente, paredes de tijolos eram construídas entre construções em complexos de apartamentos de forma que se ocorresse um incêndio o fogo não se espalharia de uma construção para outra. Estas paredes são chamamos de firewall".

Em redes de computadores, firewalls são barreiras postas entre a rede privada e a rede externa com a finalidade de evitar intrusos e ataques, ou seja, são dispositivos de segurança que protegem os recursos de hardware e de software da empresa dos perigos aos quais o sistema está exposto.

Estes mecanismos de segurança são baseados em hardware e software e seguem a política de segurança estabelecida pela empresa. O Planejamento e a implantação de um Firewall, tem como objetivo aumentar a segurança de uma empresa com conexões de redes inseguras, como por exemplo a Internet.



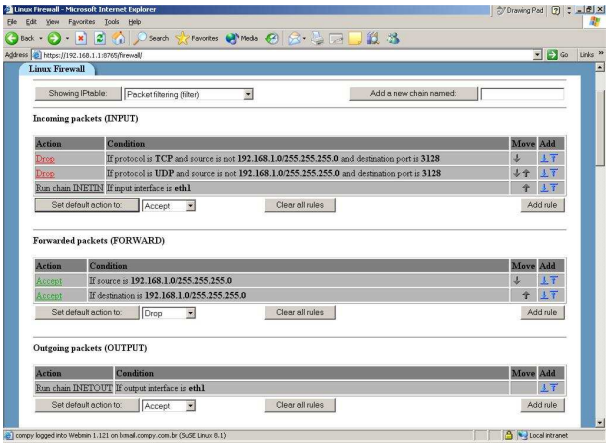
A solução de firewall cria uma barreira as tentativas de invasão.
Desta forma, não deixa passar o tráfego indesejado de informações e faz com que os serviços ou dados sejam acessados somente a partir da rede por pessoas autorizadas.
São estabelecidas regras, definidas estrategicamente, no equipamento que será usado como porta de entrada e saída para a Internet.
Em casos onde é necessário oferecer serviços para o público, como por exemplo www, ftp, webmail, entre outros, a solução de segurança permitirá separar estes serviços, em uma área chamada de zona desmilitarizada ou DMZ. Isto estabelecerá um controle sobre o acesso aos serviços públicos, sem prejudicar a rede interna.

Gerenciamento

O processo de gerenciamento está diretamente ligado aos registros feitos pelo servidor no decorrer de seu uso. Com base nesses registros o administrador é advertido sobre tentativas de invasões e necessidade de quaisquer mudanças na política de segurança da empresa.

Para facilitar o gerenciamento, o uso do IDS – que detecta as tentativas de invasão é recomendável, isso evita a necessidade de filtragem manual dos logs (registrados). A análise destas informações será de grande valia para o administrador.

Para empresas que precisam de segurança com alta confiabilidade e com baixo custo esta é uma ótima solução.



Características

- O sistema de firewall é uma parte integrante do sistema operacional, não um pacote adicional à este, isto permite o bloqueio ou o tráfego de pacotes conforme regras previamente estabelecidas;
- Registra em log toda ocorrência de bloqueio, informando a origem e o destino de cada ocorrência;
- As regras são adicionadas ou removidas imediatamente ao comando de aplicar;
- Podem ser feitos bloqueios por URL, endereços IP ou portas;
- Permite uso de NAT (Network Address Translation);
- Permite o redirecionamento de Portas e endreços;
- Permite extensões para filtragens especiais, principalmente contra ataques de hackers;
- Permite uso de proteção contra pacotes danificados ou suspeitos.

Vantagens

- Monitora todo acesso à rede;
- Suporta diversas normas de segurança. Com isso, o administrador pode estabelecer normas e disponibilizar ou bloquear serviços e informações;
- Permite que a empresa controle o acesso à Internet de seus funcionários através de senhas de acesso;
- Permite que toda a rede corporativa fique escondida atrás de um único endereço IP, tornando-a virtualmente invisível para o mundo externo, preservando a transparência no acesso à Internet;
- Permite que a empresa bloqueie sites através de filtros de URL;
- Roteamento dinâmico de pacotes;
- Como as regras são parte do sistema operacional tem alto desempenho;
- Configuração conforme política de segurança estabelecida pela empresa.

Benefícios

- Segurança;
- Confiabilidade;
- Alto desempenho;
- Simplicidade de gerenciamento para administradores;
- Versatilidade e Flexibilidade;
- Facilidade de uso pela Web;
- Baixo custo.