ARQUITETURAS DE FIREWELL
RESUNO

Universidade Federal de Santa Maria - UFSM
Graduação em Sistemas de Informação
Departamento de Tecnologia da Informação- DTecInf

Juliana de Fátima da Silva [1]; Diego de Abreu Porcellis[2].

[1]Aluno (s) voluntário (s) de extensão, Universidade Federal de Santa Maria (UFSM);
[2] Docente orientador (UFSM).

Resumo: Há basicamente três tipos de arquiteturas de firewell e mais uma que foram objetos de estudo neste trabalho. A Arquitetura **Dual-Homed Host** que para este tipo há um computador chamado **dual-homed host** que fica entre uma rede interna e a rede externa - normalmente, a internet. O nome se deve ao fato de este host possuir ao menos duas interfaces de rede, uma para cada lado, para este não há um caminho de comunicação, portanto, todo o tráfego passa por este firewall, não havendo acesso da rede interna para a rede externa (e vice-versa) diretamente. Sua vantagem é o controle elevado de trafico. A desvantagem com maior abrangência, é que qualquer problema com o dual-homed - por exemplo uma invasão - pode pôr em risco a segurança da rede ou mesmo paralisar o tráfego. Por esta razão, o seu uso pode não ser adequado em redes cujo acesso à internet é necessário. Este tipo de arquitetura é bastante utilizado para firewalls do tipo proxy. Já na arquitetura **Screened Host** há duas maquinas: uma que faz o papel de roteador (*screening router*) e outra chamada de *bastion host*. O bastion host atua entre o roteador e a rede interna, não permitindo comunicação direta entre ambos os lados. Há uma camada extra de segurança: a comunicação ocorre no sentido *rede interna - bastion host - screening router - rede externa* e vice-versa. Ainda na arquitetura Screened Host O roteador normalmente trabalha efetuando filtragem de pacotes, sendo os filtros configurados para redirecionar o tráfego ao bastion host. Este, por sua vez, pode decidir se determinadas conexões devem ser permitidas ou não, mesmo que tenham passado pelos filtros do roteador. Sendo o ponto crítico da estrutura, o bastion host precisa ser bem protegido, do contrário, colocará em risco a segurança da rede interna

ou ainda poderá torná-la inacessível. E a **Screened Subnet** também conta com a figura do bastion host, mas este fica dentro de uma área isolada de nome interessante: a *DMZ*, sigla para *Demilitarized Zone* - Zona Desmilitarizada. A DMZ, fica entre a rede interna e a rede externa, entre a rede interna e a DMZ há um roteador que normalmente trabalha com filtros de pacotes. Além disso, entre a DMZ e a rede externa há outro roteador do tipo. Esta arquitetura se mostra bastante segura, uma vez que, caso o invasor passe pela primeiro roteador, terá ainda que lidar com a zona desmilitarizada. Esta inclusive pode ser configurada de diversas formas, com a implementação de proxies ou com a adição de mais bastion hosts para lidar com requisições específicas, por exemplo. O nível segurança e a flexibilidade de configuração fazem da Screened Subnet uma arquitetura normalmente mais complexa e, consequentemente, mais cara. Estas três arquiteturas citadas anteriormente são as arquiteturas que aparecem nos livros e posts na internet, mas ainda existe a arquitetura de **Firewell Corporativo** que vamos falar agora. Conheça cada tipo a seguir: O firewall que trabalha na **filtragem de pacotes** é muito utilizado em redes pequenas ou de porte médio. Por meio de um conjunto de regras estabelecidas, esse tipo de firewall determina que endereços IP e dados possam estabelecer comunicação e/ou transmitir/receber dados. Alguns sistemas ou serviços podem ser liberados completamente (por exemplo, o serviço de e-mail da rede), enquanto outros são bloqueados por padrão, por terem riscos elevados (como softwares de mensagens instantâneas, tal como o MSN). O grande problema desse tipo de firewall, é que as regras aplicadas podem ser muito complexas e causar perda de desempenho da rede ou ter a eficácia o suficiente. Este tipo se restringe a trabalhar nas camadas TCP/IP, decidindo quais pacotes de dados podem passar e quais não. Tais escolhas são regras baseadas nas informações endereço IP remoto, endereço IP do destinatário, além da porta TCP usada. Quando devidamente configurado, esse tipo de firewall permite que somente “computadores conhecidos troquem determinadas informações entre si e tenham acesso a determinados recursos”. Um firewall assim, também é capaz de analisar informações sobre a conexão e notar alterações suspeitas, além de ter a capacidade de analisar o conteúdo dos pacotes, o que permite um controle ainda maior do que pode ou não ser acessível. E o Firewall de **controle de aplicação**

(exemplos de aplicação: SMTP, FTP, HTTP, etc.) são instalados geralmente em computadores servidores e são conhecidos como Proxy. Este tipo não permite comunicação direta entre a rede e a Internet. Tudo deve passar pelo firewall, que atua como um intermediador. O Proxy efetua a comunicação entre ambos os lados por meio da avaliação do número da sessão TCP dos pacotes. Este tipo de firewall é mais complexo, porém muito seguro, pois todas as aplicações precisam de um Proxy. Caso não haja, a aplicação simplesmente não funciona. Em casos assim, uma solução é criar um "Proxy genérico", através de uma configuração que informa que determinadas aplicações usarão certas portas. Essa tarefa só é bem realizada por administradores de rede ou profissionais de comunicação qualificados. O firewall de aplicação permite um acompanhamento mais preciso do tráfego entre a rede e a Internet (ou entre a rede e outra rede). É possível, inclusive, contar com recursos de log e ferramentas de auditoria. Tais características deixam claro que este tipo de firewall é voltado a redes de porte médio ou grande e que sua configuração exige certa experiência no assunto.

Fonte: O que é firewall? - Conceito, tipos e arquiteturas - Disponível em: <http://www.infowester.com/firewall.php>. Acesso em 28-11-2015.

Fonte: Firewall Corporativo. Acesso em: <http://www.metodotelecom.com.br/solucoes/seguranca-da-informacao/firewall-corporativo> . Acesso em 28-11-2015.