Segurança de redes com IPS, sua relação com IDS e sua importância no trabalho conjunto com o Firewall

Carlos W. Ferreira

carloswferreira@gmail.com

Abstract. *This article aims to demonstrate the importance of implementation of the IPS on corporate networks as an additional safety factor and also as essential tool to mitigate attacks and unauthorized access. The Firewall is very important in the network security, with it is possible to protect the network from unauthorized access, manage incoming and outgoing data through the network access policies, but this important tool can be quite optimized if implemented with an intrusion and detection protection system.*

Resumo. *Este artigo visa demonstrar a importância da implementação do IPS nas redes corporativas como fator adicional de segurança e também como ferramenta imprescindível para a mitigação de ataques e acessos não autorizados. O Firewall é bastante importante na segurança de redes, com ele é possível proteger a rede de acessos não autorizados, administrar o tráfego de entrada e saída de dados da rede através de políticas de acesso, porém essa ferramenta tão importante pode ser bastante otimizada se implementada com um sistema de proteção e detecção de intrusão.*

1. Introdução

Ao falar em segurança de redes, não tem como deixar de mencionar o firewall, uma importante linha de defesa que permite controlar o tráfego de rede visando a proteção contra acessos não permitidos por usuários e softwares maliciosos. A ideia quando se fala de segurança em profundidade é ter não só uma linha de defesa mas várias linhas de defesa, possibilitando um cenário onde cada nível de segurança funcione de maneira incremental.

Com a evolução do firewall surgiu o IDS, sistema de detecção de intrusão que verificavam comportamentos anormais e tentativas de acesso não autorizado à rede, emitindo alertas para que fossem tomadas as devidas providências para conter os ataques. Logo em seguida surgiu o IPS, sistema de proteção de intrusão que previam não só a detecção de ataques mas também o bloqueio desses ataques.

2. A importância do Firewall

A motivação de se implantar um firewall é basicamente filtrar todo o tráfego de uma rede, controlando a entrada e saída de dados para garantir a segurança da rede.

O firewall funciona como uma ponte entre a rede interna e a rede externa viabilizando um controle de maneira mais eficiente do tráfego de dados, implementando políticas visando cada vez mais obter uma rede mais segura.

Um outro importante papel do firewall é facilitar a administração visto que ele é um concentrador das políticas de controle de acesso e com isso torna-se mais viável e eficaz a implementação de novas funcionalidades e regras tendo em vista as novas necessidades que surgirem. Com a possibilidade de uma administração centralizada, juntamente com um sistema de detecção de intrusão para monitorar eventos relacionados à segurança, o IDS, que será mencionado mais adiante, é possível ter um controle mais efetivo.

Dentre as funções do firewall podemos citar também o seu papel como tradutor de endereços de rede que não é uma função relacionada a segurança mas que não deixa de ser importante. Na sua função de tradutor, conhecida como NAT, o firewall atua mapeando endereços de rede internos para endereços na internet.

3. Características do Firewall

No firewall podemos configurar as políticas com base em várias técnicas, no caso do controle por tipo de serviço [STALLINGS 2008], as políticas são elaboradas com base no tráfego entrada e saída e estão relacionadas a serviços de rede e internet, definindo quais poderão ser acessados e os que deverão ser bloqueados.

Nesse tipo de técnica, as regras implementadas determinam quais os serviços da internet poderão ser acessados, para requisições de entrada ou saída, podendo filtrar o tráfego com base nas informações de IP e porta TCP ou UDP.

Outro tipo de técnica é o controle do tráfego por direção, nesse tipo de técnica as regras apontam quais serão as direções confiáveis de onde partirão as solicitações de serviços.

Relacionado aos serviços podemos citar também o controle do firewall por usuário, nesse caso os serviços são disponibilizados obedecendo as regras estabelecidas especificamente para cada usuário, que pode ser interno ou externo, no caso de um acesso externo normalmente será fornecido por meio de uma autenticação segura.

4. Tipos de Firewalls

Nos firewalls de primeira geração ou firewall de filtragem de pacotes, é aplicado um conjunto de regras que tratarão o pacote com base no seu IP de origem e destino, porta TCP ou UDP de origem e destino e interface de origem de destino. Com essas

informações e também com base nas regras configuradas para controle do tráfego, o firewall irá definir se os pacotes serão encaminhados ou descartados.

Nos firewalls de segunda geração ou firewall de inspeção de estado, são restringidos os acessos às novas conexões, tráfegos que não foram originados da rede protegida e pacotes com números de sequência incorretos.

Firewalls de terceira geração ou gateway de aplicação é um outro tipo de firewall, atua como retransmissor de tráfego a nível de aplicação, recebendo requisições de uma aplicação TCP/IP, como FTP, e após o usuário informar ao gateway informações autênticas como o host remoto a ser acessado e um ID de usuário válido, com base nas regras definidas e na identificação do usuário e da aplicação, o firewall decidirá se a requisição será encaminhada.

A vantagem desse tipo de firewall e o motivo que o torna mais seguro que o firewall por filtragem de pacotes, é o fato dele ter a capacidade de controlar o tráfego através de regras que gerenciam bloqueios e permissões de recursos a nível de aplicação e não nas combinações de TCP/IP que deveram ser acessadas ou bloqueadas.

5. Limitações do Firewall

Uma das limitações do Firewall que é importante citar [STALLINGS 2008] é que o firewall não protege a rede de ameaças internas, como hosts infectados por malwares, hosts que estão realizando scan na rede sem autorização e hosts que cooperam com atacantes externos.

O firewall tem seu papel fundamental na segurança da rede, porém nos casos em que seja necessária uma ação reativa, no intuito de corrigir alguma vulnerabilidade ou cessar algum ataque que esteja ocorrendo, é necessário não apenas um firewall mas também alguma solução que analise o tráfego para verificar anomalias e indícios de ataques que estejam ocorrendo. Visando atender a essa e outras necessidades de controle e detecção de intrusão, surgiu o IDS.

6. IDS

Devido ao constante crescimento da conectividade e preocupação em ter um sistema mais eficaz de controle de tráfego, que não fosse somente baseado no método de analisar logs para perceber tráfego de dados ou hosts com comportamento fora do normal, o IDS trouxe um novo mecanismo de controle para contribuir com o trabalho do firewall.

Com o IDS se tem uma detecção de intrusão reativa que funciona de maneira rápida e automática analisando possíveis intrusões e comportamentos anômalos na rede e emitindo alertas para que sejam tomadas as medidas necessárias contra possíveis ataques.

O IDS pode se comportar de várias formas [PEREIRA 2013], os IDS's baseados em assinatura analisam o payload dos pacotes que trafegam na rede atrás de padrões

pré-configurados que possam indicar um possível ataque, caso na análise do pacote for constatado que não há indícios de intenção de ataque, o tráfego desse pacote é liberado, se houver indícios de intenção de ataque, serão emitidos alertas para que sejam tomadas as medidas necessárias.

No caso do IDS baseado em anomalias [STALLINGS 2008], o IDS é configurado para passar um certo tempo observando o funcionamento da rede e todos os seus serviços, com base nessas informações o IDS terá parâmetros para analisar como a rede se comporta e qual o trafego que será considerado normal.

No modelo baseado em anomalias o problema maior é conseguir mensurar qual o tráfego que será considerado normal visto que a rede pode ampliar, as características do tráfego podem mudar de acordo com as mudanças na rede e isso pode gerar uma grande quantidade de alertas falso-positivos, com isso irá surgir a necessidade de configurar o IDS novamente em estado de observação para gerar novos perfis de tráfego normal.

Ainda sobre os modelos de IDS, podemos citar o modelo baseado em regras [STALLINGS 2008], nesse modelo a maneira como o tráfego será interpretado é definida por meios de regras pré-configuradas.

7. IPS

Um sistema de prevenção de intrusos IPS é geralmente constituído por hardware e software [PLATO 1998] instalado em linha para monitorar as atividades de uma rede no intuito de encontrar atividades maliciosas e comportamentos indesejáveis, podendo reagir em tempo real bloqueando o tráfego dos pacotes suspeitos e prevenindo a concretização de ataques.

Os sistemas de prevenção de intrusos IPS são considerados uma extensão na tecnologia IDS [HANSCHE 2004], no caso do IDS, a sua característica é monitorar o tráfego de forma passiva, detectar anomalias e gerar alarmes.

No caso do IPS, o sistema de detecção é instalado em linha com a rede e ao invés de funcionar de maneira passiva como o IDS ou controlar o tráfego endereço de origem, destino e portas como o firewall, o IPS toma suas decisões com base no conteúdo da aplicação, por isso sua importância no trabalho em conjunto com o firewall e com um sistema detecção de intrusão eficiente.

8. Tipos de IPS

Os sistemas de detecção e prevenção de intrusos podem ser classificados de várias formas, entre elas: IPS de host, IPS de Rede, IPS de Conteúdo e Rate Based IPS.

No IPS de Host, a aplicação de segurança é instalada numa máquina que já roda outras aplicações, sendo assim o IPS divide recursos de hardware com essas aplicações e funciona monitorando o tráfego e repassando as requisições confiáveis para o destino.

Num outro cenário temos o IPS de rede, que tem a capacidade de detecção e prevenção de intrusos e que está instalado num equipamento específico para essa função, nesse tipo, o equipamento de IPS pode estar instalado entre o firewall e a rede externa ou entre o firewall e a rede interna. IPS de rede é configurado especificamente para analisar, detectar e bloquear baseando-se nas regras de segurança definidas para descartar o tráfego de rede malicioso.

Um outro modelo de IPS é o de conteúdo, nesse caso o IPS trabalha analisando o conteúdo dos pacotes buscando determinadas sequências ou padrões de assinaturas, ajudando a prevenir ataques conhecidos, propagação de worms e exploração de vulnerabilidades de protocolos.

O IPS também pode ser implementado no modelo Rate Based IPS, nesse modelo o seu principal objetivo é mitigar ataques de negação de serviço DDoS [HANSCHE 2004], nesse tipo de cenário o IPS realiza o monitoramento do tráfego da rede em tempo real, armazenando dados da análise para identificar comportamentos anormais por tipo de tráfego, como por exemplo, tráfego TCP, UDP e pacotes ARP, considerando a quantidade de sessões, número de pacotes por conexão e quantidade de pacotes por portas. Quando esses limites são ultrapassados, o IPS reconhece que está acontecendo uma tentativa de ataque.

9. Técnicas de bloqueio do IPS

Entre as técnicas de bloqueio do IPS podemos citar o bloqueio na camada de enlace, nesse pode ser configurando que uma porta qualquer do switch, por onde foram originados os ataques, seja desligada administrativamente.

Na camada de transporte o IPS é capaz de gerar pacotes TCP RST para finalizar seções TCP maliciosas ou utilizar pacotes informativos ICMP como resposta a um tráfego malicioso UDP.

E por fim, na camada de aplicação o IPS tem a função de alterar os dados maliciosos de forma que ao chegar no destino não sejam mais prejudiciais.

10. Conclusão

No mundo das redes corporativas, os administradores possuem diversas ferramentas para prover um ambiente de rede cada vez mais seguro.

As redes evoluíram muito e as comunicações estão cada vez mais complexas, com isso vão surgindo novos padrões que visam garantir a conectividade, usabilidade e desempenho.

Com o grande crescimento das comunicações, cresce também a preocupação em ter uma rede que acompanhe todo esse avanço do ponto de vista da segurança. Quando se fala em segurança de redes o firewall é sempre mencionado e isso se dá pela sua presença fundamental nas redes de maneira geral.

As soluções de firewall vêm evoluindo ao longo do tempo, porém foi visto que para conseguir um ambiente de rede seguro só o firewall não era suficiente, então começaram a aparecer os primeiros conceitos de detecção de intrusão para somar ao trabalho já realizado pelo firewall e trabalhar com o conceito de análise de tráfego e geração de alertas de intrusões e indícios de ataques.

As comunicações continuaram a evoluir e foi surgindo a necessidade de não só detectar e agir de maneira reativa mas era necessário uma ferramenta que garantisse uma defesa proativa, um mecanismo que trabalhando em conjunto com o firewall pudesse ser responsável pela detecção, prevenção e bloqueio de ataques e comportamentos anômalos nas redes.

Diante dessa necessidade e com o intuito de otimizar o trabalho do firewall, surgiu o sistema de prevenção de intrusão IPS, que veio como uma otimização do IDS, promovendo a análise do tráfego de rede, detecção e bloqueio dos ataques, trabalhando em conjunto com o firewall para garantir uma segurança cada vez mais eficiente.

Referências Bibliográficas

[HANSCHE 2004] Hansche, S., Berti, J., and Hare, C. (2004), "Official (ISC)² Guide to the CISSP Exam", AUERBACH PUBLICATIONS, pp. 617-627.

[PLATO 1998] Plato, A., NetworkICE Corporation (1998), "BlackICE Guard – User Guide".

[PEREIRA 2013] Pereira, P. (2013) "IDS/IPS: Detectando Intrusos e respondendo a ataques." – Disponível em: http://www.pedropereira.net/ips-ids-o-que-e-tutorial - Visitado em Agosto/2014.

[STALLINGS 2008] Stallings, W. (2008), "Criptografia e Segurança de Redes - Princípios e Práticas".