ABSTRAKSI

IPS +IDS firewall biasa disebut dengan IDPS atau IPS saja untuk menyingkat penyebutan. IPS didesain sebagai sebuah embedded system yang membuat banyak filter untuk mencegah bermacam-macam serangan seperti hacker, worm, virus, Denial of Service (DoS) dan trafik berbahaya lainnya, agar jaringan enterprise tidak menderita banyak kerugian bahkan ketika security patch terbaru belum diterapkan. Firewall merupakan sebuah system yang menerapkan sebuah kebijakan kontrol akses yang memeriksa trafik data yang lalu lalang dan memblok paket data yang tidak sesuai dengan kebijakan keamanan. Sebuah Intrusion Detection System (IDS) memonitor performansi system atau jaringan, mencari pola tingkah laku yang tidak sesuai dengan kebijakan keamanan atau tanda-tanda serangan yang dapat dikenali, dan kemudian jika ditemukan maka IDS akan memicu alarm. Di sini, firewall akan menolak serangan yang sudah pasti/jelas, sementara trafik yang mencurigakan akan dibiarkan lewat. Di sisi lain, IDS memonitor semua data di dalam jaringan, memberitahukan administrator jaringan akan adanya serangan pada saat serangan mulai 'hidup' dan berada di dalam jaringan. Dengan kata lain, baik IDS maupun firewall tidak mampu memblokir serangan ketika intrusi benar-benar telah terjadi. Pembangunan IPS didasarkan pada sebuah modul "in-line": data melewati perangkat IPS dari satu ujung dari kanal data tunggal, hanya data yang sudah dicek dan divalidasi oleh mesin IPS yang diperbolehkan untuk lewat menuju ujung lain dari kanal data. Pada scenario ini, paket yang mengandung tanda-tanda serangan pada paket asalnya akan dibersihkan dari jaringan. Pada Penelitian kali ini Metode IPS firewall yang digunakan adalah behavioral heuristic, dimana Firewall akan melakukan pendeteksian pada awal penggunaan untuk mendapatkan clean traffic atau lalu lintas data yang bersih. Setelah mode deteksi nanti akan masuk ke mode prevention yaitu pencegahan dimana traffic yang bisa masuk selama masa pendeteksian dapat masuk saat mode pencegahan. Tetapi segala traffic yang tidak pernah lewat akan ditolak semua.

Keywords : IPS, IDS , Fortinet *behavioral heuristic*

UNIVERSITAS MERCU BUANA

http://digilib.mercubuana.ac.id/

ABSTRACT

IPS +IDS often called IDPS or IPS as abbreviation. IPS is designed as an embedded system that makes many filters to prevent various attacks such as hackers, worms, viruses, Denial of Service (DoS) and other malicious traffic, so that enterprise networks do not suffer much loss even when the latest security patches have not been implemented. A firewall is a system that implements an access control policy that checks data traffic passing and blocks data packets that are inconsistent with the security policy. An Intrusion Detection System (IDS) monitors system or network performance, looks for behavior patterns that do not comply with security policies or recognizable attack marks, and then if found, the IDS will trigger an alarm. Here, the firewall will reject a definite attack, while suspicious traffic will be allowed to pass. On the other hand, IDS monitors all data on the network, notifying network administrators of attacks when the attack starts to 'live' and is inside the network. In other words, neither the IDS nor the firewall is capable of blocking attacks when the intrusion has actually occurred. IPS development is based on an "in-line" module: data passes IPS devices from one end of a single data channel, only data that has been checked and validated by an IPS machine is allowed to pass to the other end of the data channel. In this scenario, packets containing signs of attack on the original packet will be cleared from the network. In this Research IPS firewall method used is behavioral heuristic, where Firewall will do the detection at the beginning of use to get clean traffic or clean data traffic. After the detection mode will go into prevention mode where prevention of traffic that can enter during the detection can enter during prevention mode. But any traffic that never passes will be rejected all.

Keywords : IPS, IDS , Fortinet *behavioral heuristic*

UNIVERSITAS MERCU BUANA

http://digilib.mercubuana.ac.id/