Hiểu về hệ thống ngăn ngừa xâm nhập – IPS

SD Editor
Kiến thức - 08/10/2018

IPS (Intrusion Prevention Systems – Hệ thống ngăn ngừa xâm nhập) là hệ thống theo dõi, ngăn ngừa kịp thời các hoạt động xâm nhập không mong muốn.

Chức năng chính của IPS là xác định các hoạt động nguy hại, lưu giữ các thông tin này. Sau đó kết hợp với firewall để dừng ngay các hoạt động này, và cuối cùng đưa ra các báo cáo chi tiết về các hoạt động xâm nhập trái phép trên.

Hệ thống IPS được xem là trường hợp mở rộng của hệ thống IDS, cách thức hoạt động cũng như đặc điểm của 2 hệ thống này tương tự nhau. Điểm khác nhau duy nhất là hệ thống IPS ngoài khả năng theo dõi, giám sát thì còn có chức năng ngăn chặn kịp thời các hoạt động nguy hại đối với hệ thống. Hệ thống IPS sử dụng tập luật tương tự như hệ thống IDS.

Phân loại các loại hệ thống ngăn ngừa xâm nhập

1. Hệ thống ngăn ngừa xâm nhập mạng (NIPS – Network-based Intrusion Prevention) thường được triển khai trước hoặc sau firewall.

Khi triển khai IPS trước firewall là có thể bảo vệ được toàn bộ hệ thống bên trong kể cả firewall, vùng DMZ. Có thể giảm thiểu nguy cơ bị tấn công từ chối dịch vụ đối với firewall.

Khi triển khai IPS sau firewall có thể phòng tránh được một số kiểu tấn công thông qua khai thác điểm yếu trên các thiết bị di động sử dụng VPN để kết nối vào bên trong.

2. Hệ thống ngăn ngừa xâm nhập host (HIPS – Host-based Intrusion Prevention) thường được triển khai với mục đích phát hiện và ngăn chặn kịp thời các hoạt động thâm nhập trên các host.

Để có thể ngăn chặn ngay các tấn công, HIPS sử dụng công nghệ tương tự như các giải pháp antivirus.

Ngoài khả năng phát hiện ngăn ngừa các hoạt động thâm nhập, HIPS còn có khả năng phát hiện sự thay đổi các tập tin cấu hình.

Lý do cần triển khai IPS

Mỗi thành phần tham gia trong kiến trúc mạng đều có chức năng, điểm mạnh, điểm yếu khác nhau. Sử dụng, khai thác đúng mục đích sẽ đem lại hiệu quả cao. IPS là một trong những thành phần quan trọng trong các giải pháp bảo vệ hệ thống. Khi triển khai có thể giúp hệ thống:

- Theo dõi các hoạt động bất thường đối với hệ thống.
- Xác định ai đang tác động đến hệ thống và cách thức như thế nào, các hoạt động xâm nhập xảy ra tại vị trí nào trong cấu trúc mạng.
- Tương tác với hệ thống firewall để ngăn chặn kịp thời các hoạt động thâm nhập hệ thống.

Ưu điểm, hạn chế của hệ thống ngăn ngừa xâm nhập

Ưu điểm:

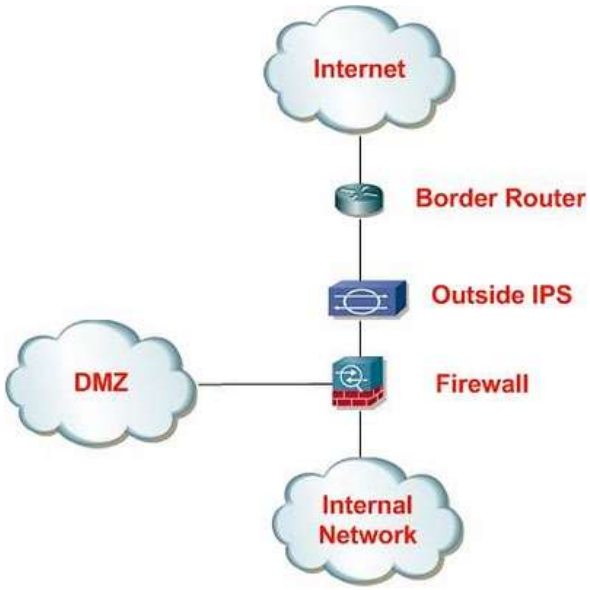
- Cung cấp giải pháp bảo vệ toàn diện hơn đối với tài nguyên hệ thống.
- Ngăn chặn kịp thời các tấn công đã biết hoặc chưa được biết.

Hạn chế:

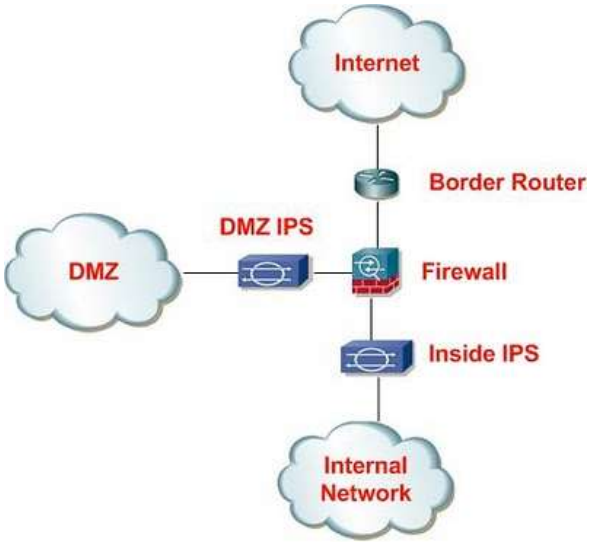
- Có thể gây ra tình trạng phát hiện nhầm (faulse positives), có thể không cho phép các truy cập hợp lệ tới hệ thống.

Thiết kế mô hình mạng

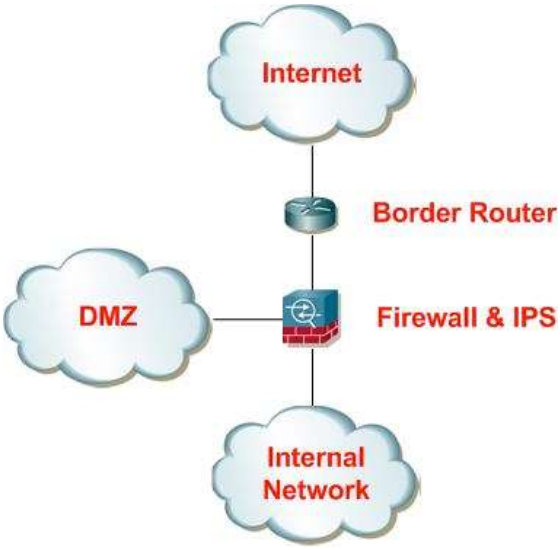
1. **Đặt trước firewall:**



2. Đặt giữa firewall và miền DMZ



3. Là một module trong giải pháp UTM



Một số tiêu chí triển khai

- Xác định công nghệ IDS/IPS đã, đang hoặc dự định triển khai.
- Xác định các thành phần của IDS/IPS.
- Thiết đặt và cấu hình an toàn cho IDS/IPS.
- Xác định vị trí hợp lý để đặt IDS/IPS.
- Có cơ chế xây dựng, tổ chức, quản lý hệ thống luật (rule).
- Hạn chế thấp nhất các tình huống cảnh báo nhầm (false positive) hoặc không cảnh báo khi có xâm nhập (false negative).

SD Editor