Kelompok 5 (S1IF-09-01)

1) Feri Yasin (21102080)
2) Satriya Yoga Madhasatya (21102087)
3) Eko Yudo Prayitno (21102111)
4) Markus Wahid Sabel Hansen Situmorang (21102133)
5) Syaloom Zefanya Yuni Br Manurung (21102036)
6) Rafli Bayu Pratama (21102021)
7) Maulidia Ramadanti (21102026)

1. Pengertian Network-Based IPS

Network-Based Intrusion Prevention System (IPS) adalah sistem keamanan jaringan yang ditempatkan pada jaringan untuk mendeteksi, mencegah, dan merespons terhadap ancaman atau serangan siber. Network-Based IPS bekerja secara real-time untuk mengidentifikasi aktivitas mencurigakan atau berbahaya pada jaringan sebelum mencapai perangkat atau server yang dilindungi.

2. Fungsi dan Tujuan Network-Based IPS

Network-Based IPS bertujuan untuk:

- Mencegah intrusi atau serangan dari luar jaringan.
- Mengidentifikasi dan menonaktifkan ancaman di jaringan sebelum mencapai endpoint atau data sensitif.
- Memberikan perlindungan lapis tambahan terhadap serangan yang tidak dapat diatasi oleh firewall atau antivirus.
- Memantau dan melacak aktivitas jaringan yang tidak wajar.
- Mengurangi risiko kerugian yang diakibatkan oleh aktivitas mencurigakan atau serangan siber.

3. Cara Kerja Network-Based IPS

Cara kerja Network-Based IPS dapat dibagi menjadi beberapa tahap utama, yaitu:

- **Monitoring Jaringan**: IPS akan memantau lalu lintas jaringan untuk mengidentifikasi aktivitas yang mencurigakan atau tidak biasa.
- **Analisis dan Deteksi**: IPS menggunakan berbagai metode analisis seperti:
    - **Signature-based Detection**: Mencocokkan pola serangan yang sudah diketahui atau tanda tangan (signature) dengan lalu lintas jaringan.
    - **Anomaly-based Detection**: Mendeteksi pola lalu lintas jaringan yang tidak normal atau tidak sesuai dengan baseline.
    - **Policy-based Detection**: Mengidentifikasi lalu lintas jaringan yang melanggar aturan kebijakan keamanan.

    - **Behavior-based Detection**: Mengamati perilaku lalu lintas untuk mendeteksi aktivitas yang tidak biasa.
- **Respons**: Setelah ancaman teridentifikasi, IPS akan merespons dengan cara-cara berikut:
    - **Blocking**: Mencegah paket data yang mencurigakan atau berbahaya masuk ke jaringan.
    - **Resetting Connection**: Menghentikan koneksi berbahaya untuk memutuskan serangan.
    - **Alerting**: Memberikan peringatan kepada administrator jaringan tentang ancaman yang terdeteksi.
    - **Logging**: Merekam semua aktivitas dan insiden sebagai log untuk kebutuhan analisis dan audit.
- **Mitigasi dan Pencegahan**: IPS memberikan langkah pencegahan agar serangan yang sama tidak terulang. Hal ini mencakup pembaruan signature, penyempurnaan kebijakan, dan analisis ancaman secara berkala.

4. Komponen Utama Network-Based IPS

Network-Based IPS memiliki beberapa komponen utama, yaitu:

- **Sensor**: Sensor ditempatkan pada berbagai titik dalam jaringan untuk mendeteksi ancaman. Sensor ini bertanggung jawab untuk memindai lalu lintas dan menerapkan metode deteksi.
- **Console**: Console adalah tempat bagi administrator untuk mengelola, memantau, dan melakukan konfigurasi pada IPS. Console sering kali berupa dashboard yang menyediakan laporan dan statistik mengenai ancaman yang ditemukan.
- **Database Signature**: Database ini berisi daftar tanda tangan ancaman yang telah diketahui dan diperbarui secara berkala. Dengan basis data yang lengkap, IPS dapat lebih cepat mendeteksi ancaman yang memiliki pola atau tanda tangan tertentu.
- **Policy Engine**: Komponen ini mengatur kebijakan keamanan yang diterapkan dalam jaringan dan mengontrol bagaimana IPS merespons ancaman.

5. Jenis-jenis Deteksi Pada Network-Based IPS

Network-Based IPS dapat melakukan deteksi melalui beberapa metode berikut:

- **Signature-based Detection**: IPS mencocokkan pola atau tanda tangan tertentu dengan lalu lintas jaringan untuk mengidentifikasi ancaman yang sudah diketahui.
- **Anomaly-based Detection**: IPS mendeteksi aktivitas abnormal dengan membandingkan lalu lintas jaringan saat ini dengan profil jaringan yang biasanya.
- **Behavioral-based Detection**: Mendeteksi perilaku atau aktivitas yang tidak biasa pada jaringan, yang mungkin menunjukkan adanya ancaman baru atau zero-day attack.

- **Heuristic-based Detection**: Menggunakan aturan dan algoritma tertentu untuk mendeteksi pola yang mencurigakan berdasarkan pengalaman atau prediksi.

6. Kelebihan dan Kekurangan Network-Based IPS

Kelebihan:

- Memberikan perlindungan real-time terhadap ancaman.
- Mengurangi dampak dari serangan yang tidak terdeteksi oleh firewall atau antivirus.
- Mencegah ancaman sebelum mencapai perangkat endpoint atau server.
- Dapat mengidentifikasi ancaman yang menggunakan enkripsi untuk menyembunyikan lalu lintas berbahaya.
- Hemat Biaya: IPS adalah cara yang hemat biaya untuk melindungi jaringan Anda dibandingkan dengan biaya menangani akibat pelanggaran keamanan

Kekurangan:

- Membutuhkan konfigurasi dan pemantauan yang baik, terutama pada jaringan dengan lalu lintas tinggi.
- Bisa memicu false positive atau peringatan palsu yang memerlukan verifikasi manual.
- Memerlukan pemeliharaan berkelanjutan dan pembaruan database signature untuk mendeteksi ancaman terbaru.

7. Perbandingan dengan Network-Based IDS

Network-Based IPS berbeda dari Network-Based Intrusion Detection System (IDS), meskipun keduanya sering digunakan bersama. Berikut adalah perbandingan antara keduanya:

Aspek	**Network-Based IDS**	**Network-Based IPS**
Fungsi Utama	Mendeteksi dan memberikan peringatan	Mendeteksi, memberikan peringatan, dan mencegah
Respons	Tidak melakukan pencegahan	Mencegah ancaman secara langsung
Posisi di Jaringan	Passive (hanya memantau)	Active (memantau dan memblokir)
Resiko False Positive	Cenderung lebih tinggi	Lebih terkendali namun tetap ada

8. Contoh Penggunaan Network-Based IPS

Network-Based IPS biasanya digunakan dalam:

- **Jaringan Perusahaan**: Untuk melindungi data sensitif dari serangan eksternal dan internal.
- **Jaringan Perbankan**: Mencegah pencurian data dan pelanggaran keamanan dalam transaksi online.
- **Jaringan Pemerintah**: Melindungi infrastruktur kritis dan data sensitif dari spionase atau serangan siber.
- **Jaringan Cloud**: Memastikan keamanan data dan aplikasi yang dihosting di cloud dengan menyediakan lapisan perlindungan terhadap ancaman yang masuk dari jaringan publik.

9. Best Practices dalam Menggunakan Network-Based IPS

1) **Update Database Signature Secara Berkala**: Pastikan tanda tangan ancaman selalu diperbarui agar dapat mengenali ancaman terbaru.
2) **Konfigurasi Kebijakan yang Tepat**: Sesuaikan kebijakan IPS dengan kebutuhan dan karakteristik jaringan perusahaan.
3) **Monitoring Secara Real-Time**: Lakukan pemantauan jaringan secara terus menerus untuk mengidentifikasi ancaman dengan cepat.
4) **Analisis dan Tindak Lanjut Insiden**: Setelah ancaman terdeteksi dan dicegah, lakukan analisis untuk mencari tahu sumber dan metode serangan yang digunakan.
5) **Pelatihan dan Edukasi Pengguna**: Edukasi pengguna dan administrator mengenai praktik terbaik untuk mengurangi risiko ancaman.

10. Kesimpulan

Network-Based IPS merupakan komponen keamanan jaringan yang sangat penting dalam infrastruktur TI modern. Dengan mendeteksi dan mencegah ancaman sebelum mencapai endpoint atau data sensitif, IPS memberikan perlindungan tambahan terhadap serangan siber. Integrasi IPS dengan sistem keamanan lainnya, seperti firewall dan IDS, dapat memberikan lapisan perlindungan yang lebih komprehensif untuk menghadapi berbagai macam ancaman siber yang terus berkembang.

Source/Sumber :

https://www.geeksforgeeks.org/intrusion-prevention-system-ips/
https://www.ibm.com/topics/intrusion-prevention-system
https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips
https://www.fortinet.com/resources/cyberglossary/what-is-an-ips
https://www.eccouncil.org/cybersecurity-exchange/network-security/ids-and-ips-differences/
https://softwarelab.org/blog/what-is-ips/