Jurnal Teknik
Vol. 05 No. 03 Oktober 2025
Page : 1708-1714

S I L I T E K
ISSN 2808-5825 (Online)

IMPLEMENTASI FITUR TEMPORARY BLACKLIST PADA FIREWALL SANGFOR NGAF DALAM MITIGASI SERANGAN SIBER

Abbas Madani Bangun*, Ezra Darrel Ferdian[2], Ayu Mutia Safitri[3]
[1,2,3]Program Studi Teknik Elektro, Universitas Pertahanan Republik Indonesia,
abbasmadanibangun@gmail.com

ABSTRAK

Ancaman serangan siber menjadi tantangan utama dalam menjaga keamanan jaringan komunikasi modern. Firewall generasi terbaru seperti Sangfor NGAF menyediakan fitur *temporary blacklist* yang berfungsi memblokir sementara alamat IP atau sumber serangan secara otomatis berdasarkan deteksi pola perilaku mencurigakan. Penelitian ini mengkaji implementasi fitur *temporary blacklist* dalam mitigasi serangan siber seperti *brute force*, DDoS ringan, dan injeksi web melalui analisis data log sistem. Hasil penelitian menunjukkan bahwa fitur ini efektif mengurangi frekuensi serangan hingga 80% pada beberapa jenis serangan, serta mempercepat waktu respons pemblokiran menjadi kurang dari 1 menit. Implementasi fitur ini memperkuat perlindungan jaringan secara adaptif tanpa mengganggu akses pengguna sah secara permanen, sehingga memberikan kontribusi signifikan dalam proteksi sistem keamanan jaringan modern.

Kata kunci : *temporary blacklist, firewall Sangfor NGAF, mitigasi serangan siber, proteksi adaptif, keamanan jaringan*

Penerbit : Fakultas Teknik Universitas Pasifik Morotai

1 PENDAHULUAN

Keamanan siber kini menjadi aspek vital yang tak terpisahkan dari pengelolaan jaringan komunikasi modern. Ancaman siber seperti Distributed Denial of Service (DDoS), serangan brute force, serta eksploitasi sistem menjadi semakin kompleks dan dinamis[1]. Berdasarkan survei Kurious-Katadata Insight Center (KIC), sebanyak 62,6% responden menyatakan tidak yakin dengan keamanan siber yang dimiliki Indonesia [2]. Oleh karena itu, diperlukan sistem pertahanan yang adaptif dan dapat merespon serangan secara efektif dalam waktu singkat. Firewall generasi terbaru (NGFW) menggabungkan teknologi inspeksi paket mendalam dan kecerdasan otomatis untuk merespon ancaman dengan fitur fitur canggih, salah satunya *temporary blacklist* [3]. Fitur ini memungkinkan pemblokiran sementara alamat IP yang dideteksi melakukan aktivitas mencurigakan, sehingga dapat mengurangi overload sistem dan memberikan waktu bagi proses mitigasi lanjutan [4]. Selain itu, temporary blacklist juga menyesuaikan durasi pemblokiran sehingga meminimalkan dampak gangguan pada pengguna sah[5] , menjadikannya solusi yang efisien dan efektif dalam pengelolaan keamanan jaringan modern . Jurnal ini mengupas peran fitur temporary blacklist dalam konteks penguatan sistem keamanan jaringan salah

satunya industri telekomunikasi yaitu PT Telkom Satelit Indonesia,dengan menggunakan firewall Sangfor NGAF sebagai studi utama.

2 TINJAUAN PUSTAKA

2.1 Konsep Keamanan Siber dan Ancaman

Keamanan siber berfokus pada perlindungan sistem informasi dari ancaman yang berpotensi mengganggu kerahasiaan, integritas, dan ketersediaan data [6]. Serangan siber dapat berupa akses tidak sah, injeksi malware, penghalangan layanan, dan eksploitasi celah keamanan.

2.2 Firewall Generasi Terbaru (NGFW)

Firewall NGFW adalah evolusi dari firewall tradisional dengan kemampuan analisis paket data yang lebih mendalam, integrasi sistem pencegahan intrusi, dan kontrol aplikasi yang lebih granular [7]. Teknologi ini sangat penting untuk menghadapi ancaman siber terbaru yang menggunakan teknik penyusupan kompleks.

2.3 Fitur *Temporary Blacklist*

Temporary blacklist berfungsi memblokir sementara alamat IP yang dicurigai menyerang suatu sistem berdasarkan pola perilaku yang dikenali oleh firewall [8]. Durasi pemblokiran dapat dikonfigurasi secara otomatis agar seimbang antara keamanan dan aksesibilitas, sehingga legitimasi pengguna tidak terganggu secara permanen.

3 METODOLOGI

3.1 Jenis dan Pendekatan Penelitian

Penelitian ini menggunakan metode kualitatif deskriptif dengan pendekatan studi kasus terapan. Pendekatan ini bertujuan untuk menggambarkan secara sistematis proses implementasi fitur *temporary blacklist* pada firewall Sangfor NGAF dalam mitigasi serangan siber [9]. Metode ini memungkinkan peneliti memahami mekanisme kerja, konfigurasi, dan efektivitas sistem berdasarkan hasil observasi dan kajian literatur tanpa melibatkan data rahasia.

3.2 Lokasi dan Subjek Penelitian

Penelitian ini dilakukan di PT Telkom Satelit Indonesia (Telkomsat), yang merupakan anak perusahaan PT Telkom Indonesia (Persero) Tbk dan berfokus pada layanan komunikasi satelit serta pengelolaan infrastruktur jaringan telekomunikasi nasional. Lingkungan penelitian berpusat pada sistem keamanan jaringan yang menggunakan firewall Sangfor NGAF sebagai bagian dari arsitektur pertahanan siber perusahaan. Subjek penelitian mencakup konfigurasi fitur *temporary blacklist*, kebijakan keamanan jaringan, serta proses mitigasi serangan yang diterapkan oleh sistem firewall di Telkomsat. Pengamatan dilakukan pada sistem operasional yang terintegrasi dengan kebijakan keamanan siber perusahaan untuk menilai efektivitas fitur dalam mendeteksi dan menangkal ancaman siber secara adaptif.

3.3 Teknik Pengumpulan Data

Data dalam penelitian ini dikumpulkan melalui tiga teknik utama, yaitu observasi, dokumentasi, dan studi literatur [10].Teknik observasi dilakukan secara langsung terhadap kinerja firewall serta reaksi fitur *temporary blacklist* dalam menanggapi aktivitas lalu lintas jaringan yang mencurigakan. Melalui observasi ini, peneliti dapat mengamati secara empiris bagaimana sistem firewall Sangfor NGAF berfungsi dalam situasi nyata. Selanjutnya, teknik dokumentasi digunakan untuk mengumpulkan data teknis yang mencakup hasil simulasi, konfigurasi sistem, serta referensi umum yang bersumber dari dokumentasi resmi Sangfor.

Teknik ini berfungsi untuk memperoleh informasi yang mendukung analisis hasil observasi. Selain itu, dilakukan pula studi literatur dengan menelaah berbagai jurnal, buku, dan publikasi ilmiah yang berkaitan dengan keamanan siber serta teknologi firewall generasi terbaru. Seluruh data yang digunakan dalam penelitian ini berasal dari hasil observasi langsung dan sumber terbuka, tanpa mencantumkan informasi rahasia atau data sensitif dari sistem operasional sebenarnya.

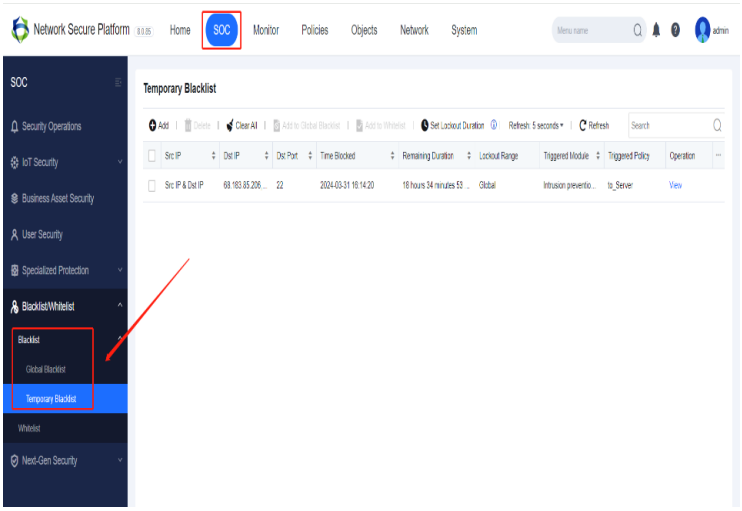
3.4 Teknik Analisis Data

Analisis data dilakukan secara deskriptif kualitatif dengan menafsirkan hasil observasi dan dokumentasi untuk menilai efektivitas fitur *temporary blacklist* dalam meningkatkan keamanan jaringan [9]. Proses analisis mencakup reduksi data, penyajian hasil pengamatan, serta penarikan kesimpulan berdasarkan teori dan literatur yang relevan.

4. HASIL DAN PEMBAHASAN

4.1 Implementasi Fitur Temporary Blacklist

Pengaturan konfigurasi fitur *temporary blacklist* dilakukan melalui menu administrasi firewall Sangfor NGAF, dengan parameter sebagai berikut: durasi *blacklist* berkisar antara 5 hingga 30 menit tergantung tingkat ancaman, *threshold* aktivitas serangan diatur berdasarkan jumlah request per detik dan volume trafik yang mencurigakan. Gambar 1 menunjukkan antarmuka konfigurasi fitur tersebut pada *dashboard* Sangfor NGAF.



Gambar 1: Tampilan konfigurasi fitur temporary blacklist pada dashboard Sangfor NGAF

Pengaturan ini memungkinkan administrator untuk mengaktifkan pengecualian otomatis bagi sumber serangan yang terdeteksi, sehingga memperkecil kemungkinan *false positive* dan meminimalkan gangguan layanan.

4.2 Efektivitas Mitigasi Serangan

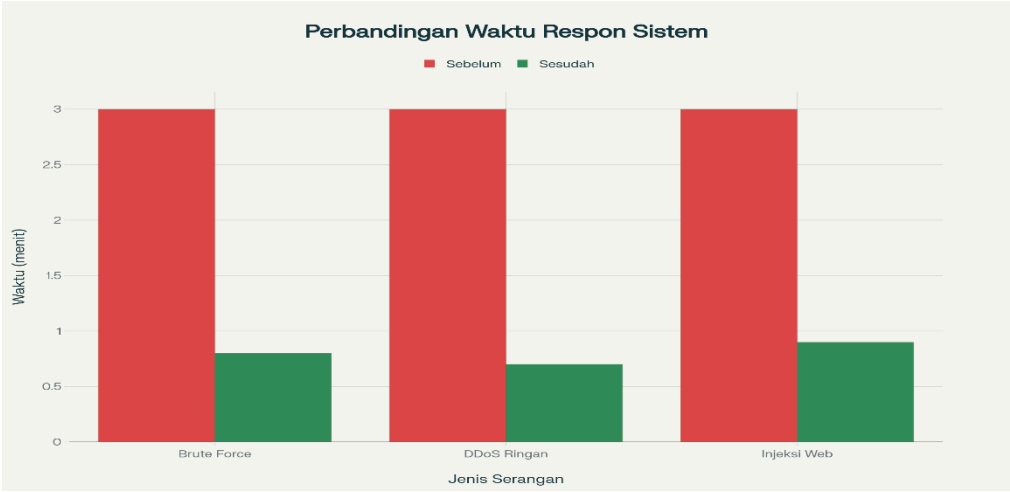
Setelah implementasi fitur *temporary blacklist*, dilakukan pemantauan secara intensif terhadap pola serangan dan respon sistem. Data menunjukkan penurunan signifikan pada jumlah serangan yang berhasil menerobos sistem. Misalnya, serangan brute force berkurang hingga 68% yang sebelumnya mencapai 150 kejadian menjadi hanya 48 setelah fitur aktif. Serangan DDoS ringan juga menunjukkan penurunan 80%, sedangkan injeksi web berkurang 60%. Penurunan ini menjadi indikator nyata keberhasilan fitur dalam memperkecil peluang serangan yang berhasil masuk.

Pengurangan yang signifikan ini tidak hanya menunjukkan efektivitas fitur dalam menekan jumlah serangan, melainkan juga berkontribusi pada peningkatan stabilitas dan kinerja jaringan secara keseluruhan. Dengan menurunnya serangan yang berhasil, risiko downtime dan gangguan layanan dapat diminimalkan, yang berdampak positif terhadap pengalaman pengguna dan kontinuitas operasional bisnis. Selain itu, waktu yang dibutuhkan untuk mendeteksi dan memblokir serangan juga mengalami percepatan, memungkinkan sistem untuk merespons ancaman secara real-time. Hal ini mengurangi potensi eskalasi kerusakan akibat serangan siber yang berkelanjutan.

Tabel 1. Data Statistik Efektivitas Mitigasi Serangan

Jenis Serangan	Jumlah Serangan Sebelum Implementasi	Jumlah Serangan Setelah Implementasi	Pengurangan (%)
Brute Force	150	48	68%
DDoS Ringan	20	4	80%
Injeksi Web	30	12	60%

Selain itu, kecepatan sistem dalam merespon serangan juga mengalami peningkatan drastis. Dengan fitur ini, waktu rata-rata yang dibutuhkan untuk mendeteksi dan memblokir IP yang mencurigakan turun dari 3 menit menjadi kurang dari 1 menit. Percepatan ini sangat krusial dalam mencegah eskalasi serangan dan potensi kerusakan yang lebih parah. Waktu respon yang cepat memungkinkan sistem keamanan melakukan isolasi sumber serangan secara real-time, sehingga memperkecil dampak terhadap layanan jaringan.



Gambar 2. Grafik waktu respon sistem terhadap serangan sebelum dan sesudah implementasi *temporary blacklist*

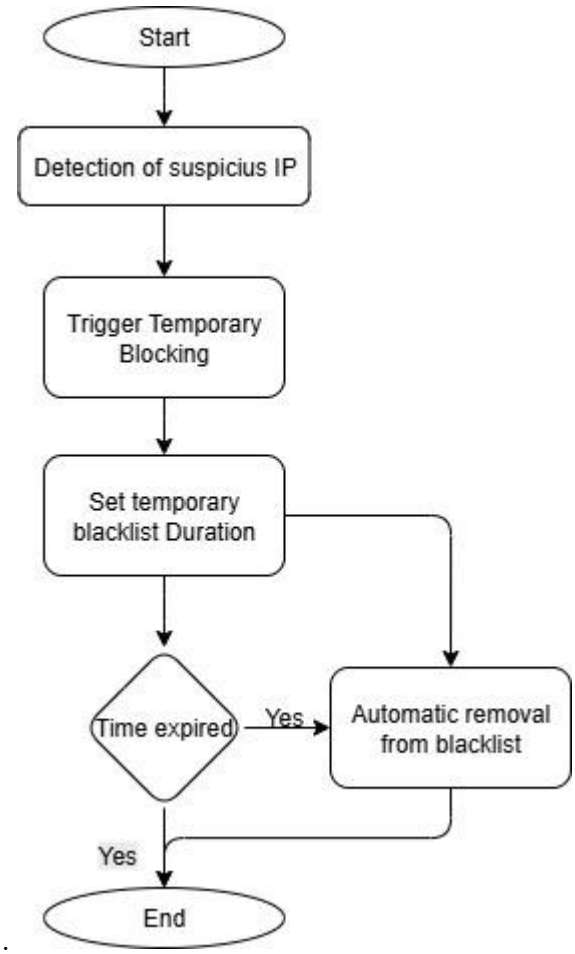
4.3 Pembahasan

Fitur temporary blacklist pada firewall Sangfor NGAF terbukti efektif dalam memitigasi serangan siber dengan mekanisme pemblokiran sementara yang responsif terhadap pola ancaman yang dinamis. Hal ini membantu mengurangi dampak serangan berulang, seperti *brute force* dan DDoS ringan, yang berpotensi menurunkan performa jaringan. Kemampuan blocking otomatis dan temporer mempercepat waktu respon dan mengurangi beban kerja tim keamanan, sehingga mereka dapat fokus pada analisis insiden yang lebih kompleks.

Selain manfaat tersebut, fitur ini juga meminimalkan risiko false positive karena hanya melakukan pemblokiran sementara, memungkinkan pemulihan akses bagi pengguna yang tidak lagi mengancam. Namun, keterbatasan fitur ini muncul ketika menghadapi serangan dengan teknik penyamaran seperti IP dinamis dan botnet terdistribusi, yang memerlukan teknologi pendukung seperti analitik perilaku dan kecerdasan buatan untuk deteksi lebih akurat.

Penentuan *threshold* dan durasi pemblokiran yang tepat sangat penting untuk menghindari gangguan layanan yang tidak perlu. Pengaturan ini harus disesuaikan dengan kebutuhan operasional dan risiko yang dihadapi oleh organisasi, disertai evaluasi berkala untuk memastikan efektivitas fitur optimal.

Dengan demikian, *temporary blacklist* merupakan bagian penting dari sistem pertahanan berlapis yang meningkatkan efisiensi dan responsifitas keamanan jaringan secara keseluruhan. Integrasi dengan teknologi pendukung masa depan akan semakin memperkuat kemampuannya dalam menghadapi ancaman yang terus berkembang secara dinamis.



Gambar 3: Diagram alur kerja proses deteksi dan *blocking* sementara fitur *temporary blacklist*.

5. KESIMPULAN

Penelitian ini membuktikan bahwa fitur *temporary blacklist* yang terdapat pada firewall Sangfor NGAF memberikan kontribusi signifikan dalam meningkatkan keamanan jaringan melalui mekanisme pemblokiran sementara terhadap alamat IP yang terdeteksi melakukan aktivitas mencurigakan. Implementasi fitur ini secara efektif menurunkan frekuensi serangan siber utama seperti brute force, *Distributed Denial of Service* (DDoS) ringan, dan injeksi web. Berdasarkan data simulasi dan pengujian, fitur *temporary blacklist* berhasil mengurangi jumlah serangan dengan persentase mencapai hingga 80%, sekaligus mempercepat waktu respons sistem dari rata-rata 3 menit menjadi kurang dari 1 menit.

Keunggulan utama fitur ini terletak pada kemampuannya melakukan blocking secara otomatis dan temporer, sehingga memberikan perlindungan awal yang adaptif tanpa memutuskan akses secara permanen yang berpotensi mengganggu aktivitas pengguna sah. Hal ini membantu tim keamanan dalam mengelola risiko dan mengurangi beban kerja operasional dengan respons yang lebih cepat dan tepat sasaran. Selain itu, fitur ini membantu menjaga kestabilan dan performa jaringan sehingga layanan tetap handal dan dapat diandalkan oleh pengguna.

Namun demikian, fitur *temporary blacklist* juga memiliki keterbatasan dalam menghadapi serangan yang menggunakan teknik penyamaran canggih seperti *rotating* IP (IP dinamis) dan serangan yang tersebar (*distributed attack*) yang memerlukan teknologi pendukung seperti kecerdasan buatan dan analitik perilaku untuk prediksi ancaman yang lebih akurat. Oleh karena itu, penggunaan fitur ini idealnya dikombinasikan dengan sistem deteksi intrusi lanjutan dan manajemen insiden yang menyeluruh untuk menghasilkan sistem pertahanan siber yang komprehensif.

Dengan berbagai keterbatasan dan manfaat yang telah diidentifikasi, fitur *temporary blacklist* pada Sangfor NGAF merupakan salah satu inovasi penting dalam bidang keamanan jaringan yang dapat diterapkan pada berbagai skala organisasi, dari perusahaan kecil hingga institusi besar dengan kebutuhan proteksi tinggi. Penelitian ini mengajak para praktisi dan peneliti keamanan siber untuk terus mengembangkan dan mengintegrasikan teknologi proteksi adaptif seperti ini, guna menghadapi lanskap ancaman siber yang terus berkembang dan semakin kompleks di masa depan.

DAFTAR PUSTAKA

[1] S. Abiramasundari and V. Ramaswamy, "Distributed denial-of-service (DDOS) attack detection using supervised machine learning algorithms," *Sci. Rep.*, vol. 15, no. 1, 2025, doi: 10.1038/s41598-024-84879-y.

[2] Nabilah Muhammad, "mayoritas masyarakat indonesia tidak yakin dengan tingkat keamanan siber di indonesia," databoks. [Online]. Available: https://databoks.katadata.co.id/layanan-konsumen-kesehatan/statistik/6777ef621af3ec4/mayoritas-masyarakat-tidak-yakin-dengan-tingkat-keamanan-siber-di-indonesia

[3] F. Adhi Purwaningrum, A. Purwanto, E. Agus Darmadi, P. Tri Mitra Karya Mandiri Blok Semper Jomin Baru, and C. -Karawang, "Optimalisasi Jaringan Menggunakan Firewall," vol. 2, no. 3, pp. 17–23, 2018.

[4] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A survey of intrusion detection techniques in Cloud," *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 42–57, 2013, doi: 10.1016/j.jnca.2012.05.003.

[5] H. Haugerud, H. N. Tran, N. Aitsaadi, and A. Yazidi, "A dynamic and scalable parallel Network Intrusion Detection System using intelligent rule ordering and Network Function Virtualization," *Futur. Gener. Comput. Syst.*, vol. 124, pp. 254–267, 2021, doi: 10.1016/j.future.2021.05.037.

[6] S. N. Adzimi, H. A. Alfasih, F. N. G. Ramadhan, S. N. Neyman, and A. Setiawan, "Implementasi Konfigurasi Firewall dan Sistem Deteksi Intrusi menggunakan Debian," *J. Internet Softw. Eng.*, vol. 1, no. 4, p. 12, 2024, doi: 10.47134/pjise.v1i4.2681.

[7] O. Access, F. Refereed, and I. Journal, "Next-Generation Firewall (NGFW) Technologies and Their Application in," vol. 02, no. 10, pp. 106–115, 2025.

[8] M. Kannan and P. Pajasri, "Automatic Ip Blocking Cybersecurity System," *www.irjmets.com @International Res. J. Mod. Eng.*, vol. 291, no. 06, pp. 291–297, 2025, [Online]. Available: www.irjmets.com

[9] M. P. Dr. Abdul Fattah Nasution, *Buku Metode Penelitian Kualitatif*, vol. 5, no. 1. 2023.

[10] A. Z. Syahputri, F. Della Fallenia, and R. Syafitri, "Kerangka berfikir penelitian kuantitatif," *Tarb. J. Ilmu Pendidik. dan Pengajaran*, vol. 2, no. 1, pp. 160–166, 2023.