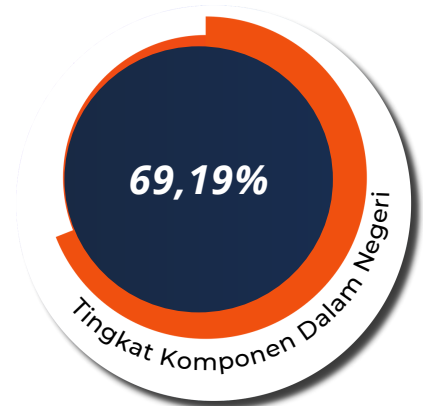


TKMT RISK MANAGEMENT NEXT GENERATION FIREWALL



TKMT Risk Management Next Generation Firewall membantu organisasi untuk melindungi jaringan dari ancaman keamanan terkini. Dengan menggunakan Produk ini dapat menghemat waktu dalam pengaturan gateway internet karna produk TKMT Risk Management telah menggunakan pengetahuan dan basis data yang dikembangkan dengan bantuan teknologi pembelajaran mesin dan kecerdasan buatan.



Kemampuan



Next-Generation Firewalls

Untuk perusahaan publik dan komersial dari berbagai ukuran dengan 50 - 10.000 pengguna Internet yang menggunakan sistem operasi seluler dan desktop apa pun.



Server VPN

Untuk koneksi kantor dan pengguna jarak jauh yang aman dan andal melalui VPN. mendukung protokol asli IKEv2/IPSec, L2TP/IPSec, SSTP. Biaya administrasi dan keamanan mumpuni untuk organisasi skala menengah



Otorisasi Pengguna

Menggunakan otorisasi Single Sign-On atau otorisasi melalui log keamanan dari pengendali domain untuk kontrol akses yang transparan dan mudah ke situs web dan sumber daya Internet.



Keamanan dan Perlindungan Email

Penyaringan spam dan phishing scam yang terpadu didalam perangkat NGFW



Server Proxy dan Filter Web

Pemfilteran lalu lintas web berdasarkan 145 kategori. Inspeksi SSL. Streaming pemeriksaan virus.



Integrasi fleksibel ke dalam Infrastruktur Jaringan Integrasi yang mudah dengan Microsoft Active Directory, SIEM (via syslog), sistem pemantauan (agen Zabbix, SNMP), DLP (via ICAP). Protokol perutean dinamis BGP, OSPF.



Pemantauan dan Pelaporan

Laporan penggunaan web yang terkelompok. Laporan situs web yang diizinkan atau diblokir. Memberikan Log waktu sesi web yang terperinci.



Center Kontrol

Memungkinkan pengelolaan berbagai kebijakan keamanan yang diterapkan pada firewall untuk menjaga keamanan jaringan. Seperti filter konten, kontrol aplikasi, batasan kecepatan.

Contacts:

www.tkm-teknologi.id






Email : support@tkm-teknologi.com

+62 811-1552-270







TKMT RISK MANAGEMENT NEXT GENERATION FIREWALL



Keuntungan

- 
Amankan Data dan infrastruktur
 - Memberikan perlindungan terhadap ransomware dan malware penambang kripto.
 - Mencegah penggunaan sumber daya kerja tanpa izin seperti akses Internet, perangkat lunak, dan situs web yang tidak relevan dengan pekerjaan.
- 
Tingkatkan Produktivitas Karyawan
 - Membatasi akses karyawan ke jaringan internet untuk konten seperti hiburan dan berita palsu, jejaring sosial, forum, dan game online yang tidak sesuai dengan tugas kerja.
 - Memblokir iklan dan spanduk yang mengalihkan perhatian karyawan, membantu mereka fokus pada pekerjaan mereka.
- 
Meningkatkan Kecepatan Efektif Saluran Internet
 - Sebagian besar lalu lintas terdiri dari lalu lintas sampah seperti torrent, telemetri Windows, spyware, spanduk, dan virus.
 - Meningkatkan efisiensi pemanfaatan saluran Internet tanpa biaya perluasan saluran.
- 
Blokir Ancaman Sebelum Terjadi
 - Sebagian besar virus di jaringan lokal berasal dari Internet.
 - Sebagian besar malware diunduh dari botnet dan berkomunikasi dengan pusat komando dan kontrol (C&C). Blokir unduhan dan pantau host yang terinfeksi dengan memantau lalu lintas di perimeter jaringan.
- 
Tingkatkan Aksesibilitas Eksternal Layanan Anda dengan Aman
 - Pastikan karyawan dapat bekerja dengan baik meskipun mereka tidak berada di kantor pusat.
 - Dapat bekerja dengan aman melalui VPN, bahkan saat melakukan perjalanan bisnis: semua tugas penting akan diselesaikan tepat waktu dan data sensitif akan tetap aman.
 - Publikasikan sumber daya web dan server email menggunakan teknologi keamanan terbaru.

Fitur Produk

- | | |
|---|---|
|  <p>Penyaringan Konten
Kontrol akses jaringan dengan memblokir 500 juta alamat dalam 145 kategori, seperti phishing/penipuan, pusat distribusi malware, botnet, pengumpulan data rahasia, spam, dan iklan/spanduk.</p> |  <p>Memblokir Anonymizer
Mencegah upaya melewati sistem pemfilteran konten menggunakan server proxy, plugin browser, TOR, dan VPN.</p> |
|  <p>Sistem Pencegahan Intrusi (IPS)
Memblokir serangan, DoS, spyware, telemetri Windows, pusat C&C botnet, penambang kripto berbahaya. Aktivitas pencegahan virus dalam jaringan. Memblokir wilayah yang tidak dapat diandalkan berdasarkan reputasi GeolP dan IP.</p> |  <p>Penerbitan Sumber Daya (WAF)
Melindungi sumber daya web internal dengan menggunakan Web Application Firewall saat mempublikasikannya di Internet, serta menyediakan pemfilteran dan perlindungan lalu lintas email untuk server email yang dipublikasikan.</p> |
|  <p>Kontrol Aplikasi (DPI)
Memungkinkan Anda memblokir lalu lintas dari Skype, WhatsApp, BitTorrent, Youtube, Steam, TikTok, dll. untuk pengguna dan grup tertentu.</p> |  <p>Pemindaian Lalu Lintas Antivirus
Streaming pemindaian file dan skrip yang diunduh menggunakan perangkat lunak Kaspersky Anti-Virus. Memblokir virus sebelum masuk ke jaringan lokal.</p> |

Contacts:

www.tkm-teknologi.id

Email : support@tkm-teknologi.com

+62 811-1552-270