



NGAF

Application Control Troubleshooting

Version 8.0.6



Perubahan Catatan

Tanggal	Deskripsi Perubahan
July 4, 2019	Application control troubleshooting.

Daftar Isi

Bab 1 Scenario Aplikasi.....	1
Bab 2 Metode Troubleshooting.....	1

Bab 1 Scenario Aplikasi

Rule application control tidak berjalan

Bab 2 Metode Troubleshooting

1. Periksa apakah URL Database dan Application Ident Database sudah di versi terbaru. Bila database belum di versi terbaru, ini bisa membuat beberapa aplikasi tidak terbaca secara benar, sangat direkomendasikan untuk mengupdate database ke versi terbaru terlebih dahulu. Kita bisa memastikan fitur identifikasi aplikasi ini dengan cara mensetting application control log event. (Masuk ke tab Policies -> Application Control dan edit policy lalu pilih advanced settings: log event)2 Product Version.

No.	Database	Current Version	Latest Version	Update Svc Expir...	Auto Update	Operation
1	File Verification Model Database	2018-11-15 Logs	2018-11-15	2020-04-09	✓	
2	URL Database	2019-06-25 Logs	2019-06-25	2020-06-10	✓	
3	Exploit Protection Database	2019-06-27 Logs	2019-06-27	2020-06-10	✓	
4	Software Update	af806_kb007_sp af806_kb006_sp af8...	af806_kb007_sp af806_kb006_sp af8...	Never expire	✓	
5	Application Ident Database	2019-06-24 Logs	2019-06-24	2020-06-10	✓	
6	WAF Signature Database	2019-06-05 Logs	2019-06-05	2020-06-10	✓	
7	Data Leak Protection	2018-02-16 Logs	2018-02-16	2020-06-10	✓	
8	Vulnerability Analysis Rule	2019-06-26 Logs	2019-06-26	2020-06-10	✓	
9	IP address database	2019-07-01 Logs	2019-07-01	Never expire	✓	
10	Threat Intelligence Database	2019-06-26 Logs	2019-06-26	Never expire	✓	
11	Hot Threat Database	2019-05-28 Logs	2019-05-28	2020-06-10	✓	
12	Security Events	2019-06-28 Logs	2019-06-28	2020-06-10	✓	

2. Masuk ke Policies -> Access Control -> Application Control lalu cek apakah Zone & Service/Application sudah di konfigurasi dengan benar. Dan pastikan policy sudah di enabled.

Priority	Name	Group	Src Zone	Dst Zone	Destination	Service/Application	Schedule	Time Updated	Action	Hit Count	Stat...	Operation
1	block quick	Default group	lan	...	Private Network...	...	All week	06-27 10:10:13	Deny	127	✓	

3. Masuk ke Policies -> Access Control -> Application Control lalu cek apakah ada policy yang invalid atau konflik.

Priority	Name	Group	Src Zone	Dst Zone	Destination	Service/Application	Schedule	Time Updated	Action	Hit Count	Stat...	Operation
1	block quick	Default group	lan	...	Private Network...	...	All week	06-27 10:10:13	Deny	127	✓	
2	Allow_all	Default group	LAN	wan	lan	10:10:13	Deny	127	✓	
3	Default Poi...	-	All	10:58:54	Allow	9999+	✓	
									Deny	0	✓	

4. Tambahkan policy baru untuk IP testing dan pindahkan policy tersebut ke paling atas agar tidak terganggu dengan policy lainnya.
5. Masuk ke Policies -> Blacklist/Whitelist cek apakah IP tersebut ada di list Whitelist. Disable semua domain name whitelist untuk mencegah terjadinya DNS Pollution.
6. Masuk ke System -> Troubleshooting lalu capture packet untuk mengkonfirmasi apakah packet melewati NGAF di kedua arah.



Hak cipta (c) Sangfor Technologies Inc. Hak cipta dilindungi oleh undang-undang. Dilarang menyebarkan atau memproduksi ulang sebagian dari atau seluruh dokumen ini tanpa persetujuan tertulis dari Sangfor Technologies Inc. SANGFOR adalah merek dagang dari Sangfor Technologies Inc. Semua merek dagang dan nama dagang lain yang disebutkan dalam dokumen ini adalah milik dari pemegangnya masing-masing. Segala upaya telah dilakukan dalam mempersiapkan dokumen ini untuk memastikan keakuratan konten, namun semua pernyataan, informasi, dan rekomendasi dalam dokumen ini bukan merupakan jaminan dalam bentuk apa pun, tersurat maupun tersirat. Informasi dalam dokumen ini dapat berubah tanpa pemberitahuan. Untuk mendapatkan versi terbaru, hubungi pusat layanan internasional SANGFOR Technologies Inc.