



NGAF

Application Control -

Version 8.0.8



Data Perubahan

Tanggal	Keterangan Perubahan
July 2, 2019	Versi 1.0 rilis dokumen.

DAFTAR ISI

BAB 1 Pengenalan.....	1
BAB 2 Penerapan Paling Efisien.....	1
1 Petunjuk Akses Jaringan pada PC.....	1
1.1 Kontrol dengan Syarat Khusus	2
2 Petunjuk Akses Jaringan pada Server	2
2.1 Kebutuhan Server mengakses Jaringan	2
2.2 Server Mengakses Jaringan Tidak Dibutuhkan	3
3 Petunjuk untuk Publikasi Layanan Server	3
3.1 Tidak menggunakan DNAT pada NGAF.....	3
3.2 Menggunakan DNAT pada NGAF	5
BAB 3 Perhatian.....	5
BAB 4 Hubungi Kami	6

BAB 1 Pengenalan

Application control policy melakukan kontrol paket data TCP/IP dari paket data interaktif atau karakteristik dari layer aplikasi (Layer 7 dari OSI layer) untuk mencegah paket data yang tidak diperbolehkan.

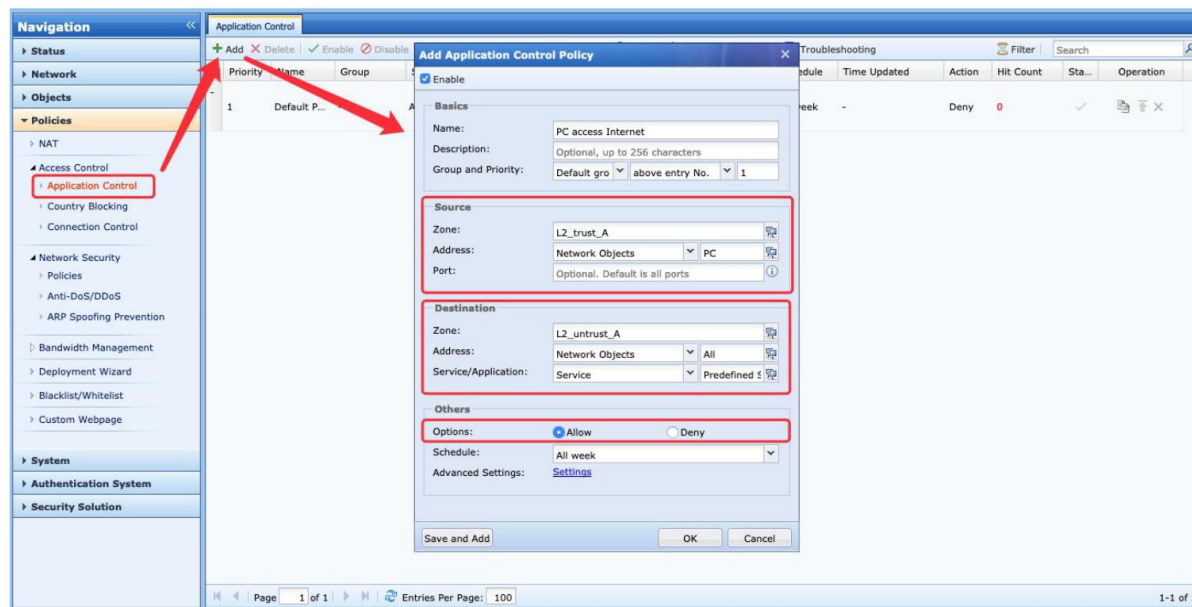
BAB 2 Penerapan Paling Efisien

Dengan menyertakan pengaturan application control, interaktif data dari kedua pihak dalam komunikasi dapat ditentukan dan dikendalikan dalam penerapan dari pembatasan hak akses, dapat menekan jangkauan dari sebuah serangan dan resiko keamanan. Saran ini hanyalah sebuah referensi, semua tergantung pada jaringan sebenarnya untuk keadaan khusus.

Catatan: Kebijakan application control pada dasarnya melakukan pembatasan terhadap perilaku akses. Mengatur paling tidak satu kebijakan “allow” untuk memastikan akses jaringan berjalan normal.

1 Petunjuk Akses Jaringan pada PC

Untuk pengguna yang tidak memiliki persyaratan kontrol secara khusus untuk akses jaringan pada PC, disarankan untuk disiapkan segmen IP dan area/Zone untuk PC dan diperbolehkan/allow mengakses jaringan (dari LAN menuju WAN) untuk semua aplikasi pada PC. Konfigurasi seperti dibawah ini.



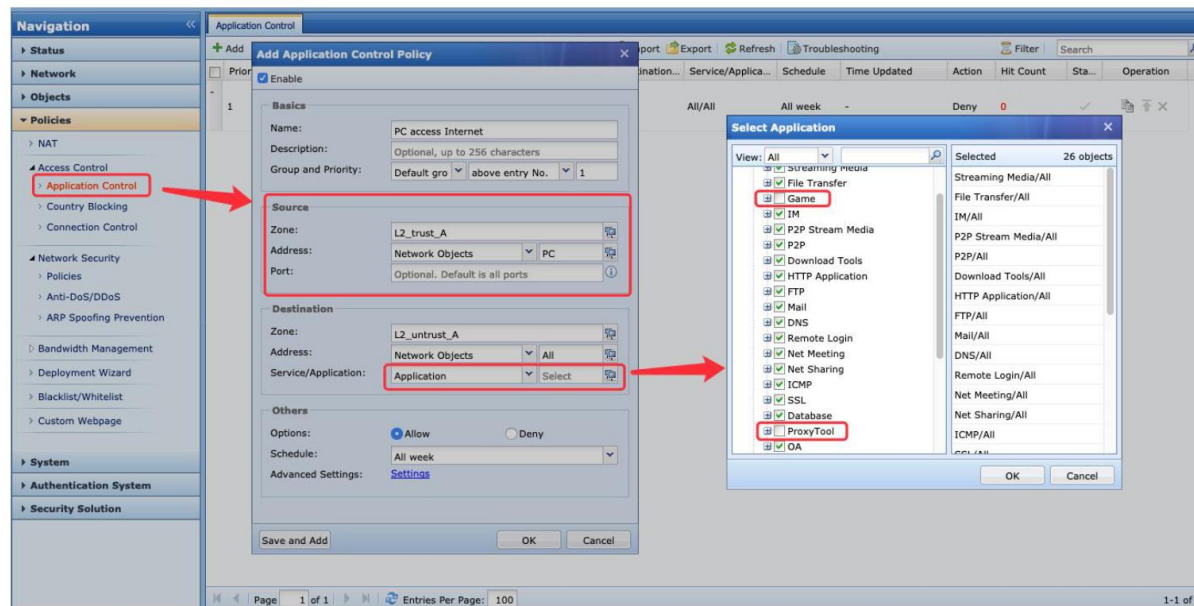
Catatan: Kebanyakan administator lebih menyukai menggunakan satu aturan/policy untuk memperbolehkan semua IP untuk mengakses jaringan dari dua-arrah/bi-direction. Penerapan ini tidak disarankan. Hanya perlu diperbolehkan untuk akses data dari LAN ke WAN jika tidak ada kebutuhan khusus pada PC.

Catatan: Harap diperhatikan pada skenario: NGAF di seting dalam mode jembatan/bridge atau virtual wire, dan koneksi WAN pada AF menggunakan DHCP server (Contoh, perangkat AF

terkoneksi dengan DHCP sebagai gateway). Pada skenario ini, diperlukan untuk memperbolehkan/allow paling tidak layanan DHCP dari WAN ke LAN: UDP port 67 & 68, untuk memastikan koneksi PC dapat mendapatkan alamat DHCP.

1.1 Kontrol dengan Syarat Khusus

Untuk pengguna yang memiliki persyaratan khusus pada PC yang mengakses jaringan (contoh, PC dapat mengakses jaringan tapi tidak boleh bermain game online atau menggunakan proxy tool). Konfigurasi seperti dibawah ini.

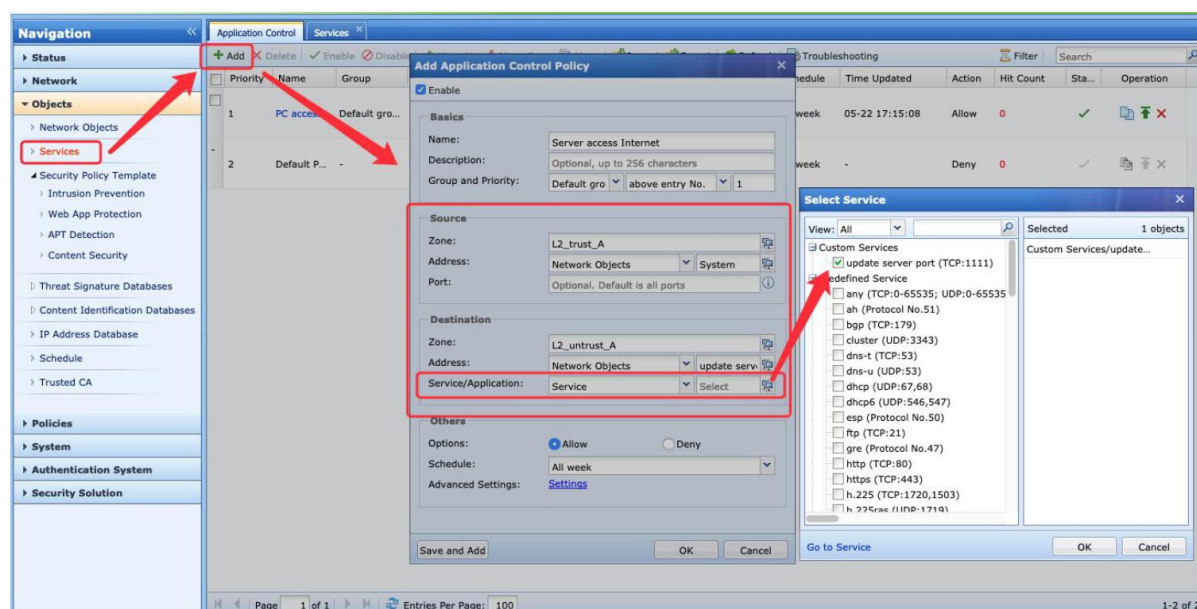
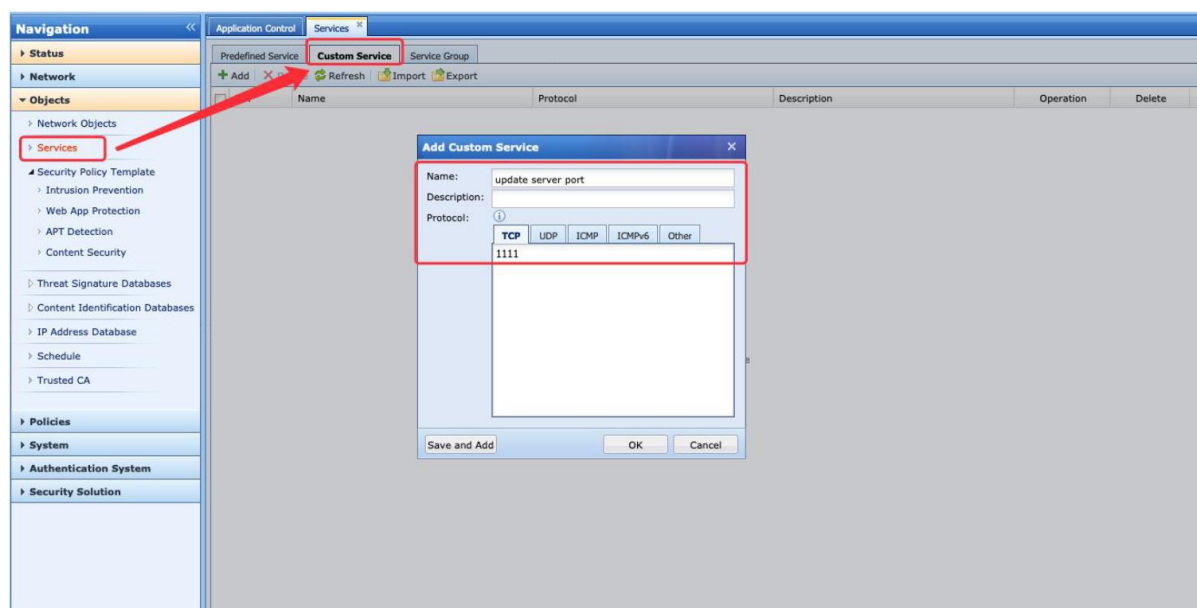


2 Petunjuk Akses Jaringan pada Server

2.1 Kebutuhan Server mengakses Jaringan

Pada umumnya ini diperlukan pada saat server memerlukan akses yang khusus, seperti pembaruan piranti/software atau sinkronisasi data pada server tertentu. Dalam situasi seperti ini disarankan untuk ditentukan terlebih dulu tujuan alamat IP yang akan diakses beserta dengan port-nya.

Contoh, Server dari portal website membutuhkan akses sinkronisasi data server yang berada pada jaringan awan/cloud secara terus menerus dengan alamat IP: 200.200.200.200:1111



2.2 Server Mengakses Jaringan Tidak Dibutuhkan

Dalam situasi ini, tidak diperlukan konfigurasi aturan/policy “Allow” untuk server menuju area/Zone WAN. Aturan dasar/default policy akan mencegah akses jaringan perilaku tidak biasa dari server

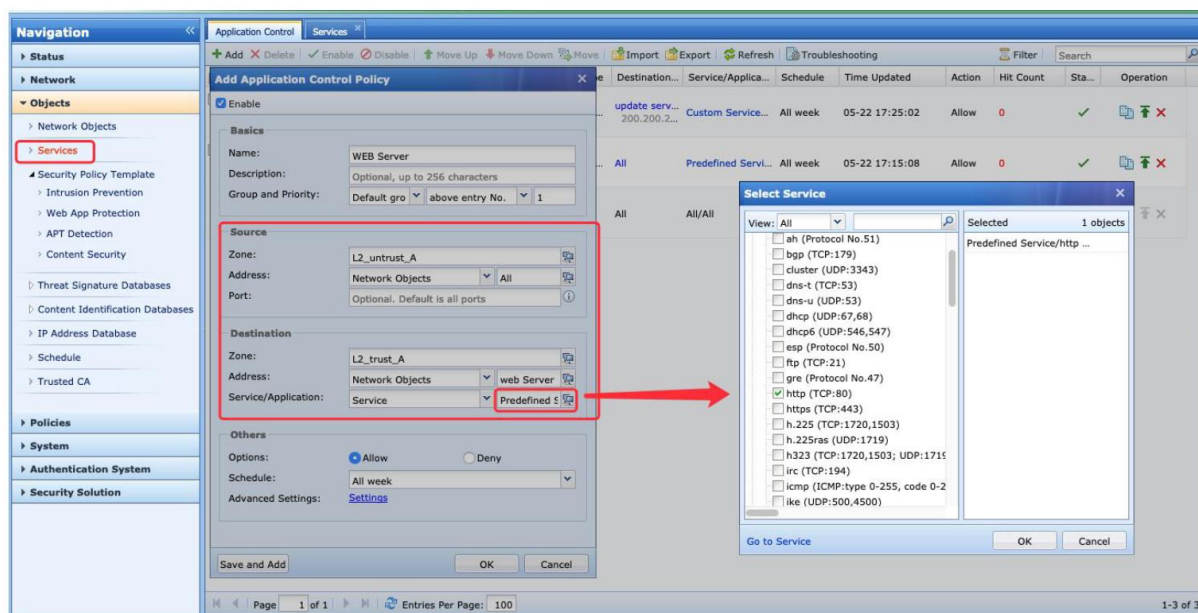
3 Petunjuk untuk Publikasi Layanan Server

3.1 Tidak menggunakan DNAT pada NGAF

Pada skenario ini relatif sederhana, Pada server hanya diperlukan port/service yang akan dipublikasi ke publik. Port/Service lainnya tidak diperbolehkan.

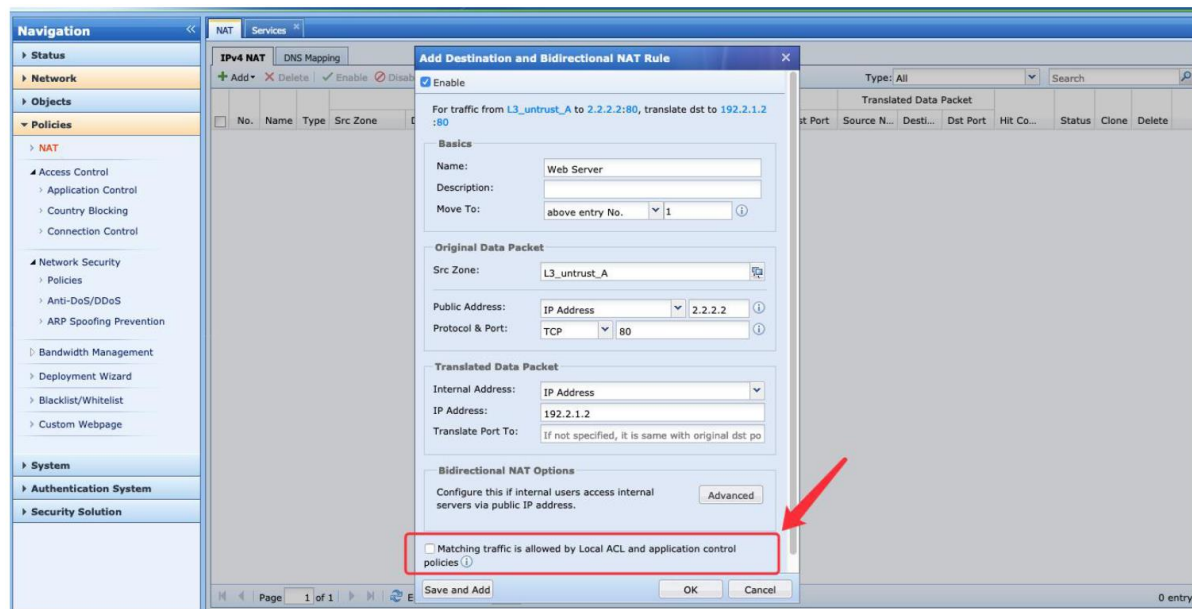
Contoh, portal website hanya memerlukan port HTTP untuk publikasi ke publik.

NGAF_v8.08_Application Control_Penerapan Paling Efisien



3.2 Menggunakan DNAT pada NGAF

Catatan pada aturan/policy DNAT, semua konten dari DNAT diperbolehkan untuk diakses berdasarkan aturan application control policies secara default. Ketika dalam keadaan pemetaan untuk publikasi IP, disarankan untuk menonaktifkan opsi ini dan mengaktifkan layanan secara manual pada application control policies.



BAB 3 Perhatian

- Harap diperhatikan saat mengaktifkan “Persistent Connection” pada [Application Control] – [Advanced Setting]. Hanya aktifkan pada server yang membutuhkannya saja (jika hanya diperlukan). Sebaiknya jangan digunakan/diaktifkan pada banyak server untuk menghindari slow release dari link pada alat, dimana dapat menyebabkan penurunan kinerja pada alat.
- Harap diperhatikan saat mengaktifkan “Logging” pada [Application Control] – [Advanced Setting]. Disarankan untuk menyimpan log pada “External Data Center” jika item dari log besar, untuk menghindari log yang tampil pada “Internal Data Center” yang terlalu banyak, dimana dapat menyebabkan penurunan kinerja pada alat.
- terdapat tiga fungsi pada [Application Control] – [Troubleshooting] : “Policy Validity Check”, “Policy Troubleshooting” and “Group Management”. Anda dapat memperkenalkan ketiga fungsi ini pada pengguna untuk penyederhanaannya dan mempermudah penggunaan fitur dari produk.

BAB 4 Hubungi Kami

Technical Support Email:	tech.support@sangfor.com
Technical Support Hotline:	International Service Centre: +60 12711 7129 (7511) Malaysia: 1700 81 7071 Hong Kong: +852 81257201 Singapore: +65 3152 9370 Other Regions: +60-12-7117511 (7129)
Technical Support Community:	http://community.sangfor.com
Official Website:	http://www.sangfor.com



Hak cipta (c) Sangfor Technologoes Inc. Hak cipta dilindungi oleh undang-undang.

Dilarang menyebarluaskan 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.