SANGFOR

NGAF

Pedoman Terbaik untuk Skenario Akses Kontrol

Versi 8.0.17

Data Perubahan

Tanggal	Keterangan Perubahan
26 Agustus 2020	Versi 8.0.17 rilis dokumen.
17 May 2021	Pembaruan Dokumen

DAFTAR ISI

BAB 1 Skenario 1

BAB 2 Pedoman Dasar 1

Pengecekan 1

Blok Aplikasi Teracak/dienkripsi 2

1 Saran Akses Jaringan pada PC 3

1.1 Dengan Kebutuhan Kontrol khusus 3

2 Saran Akses Jaringan pada Server 4

2.1 Kebutuhan Akses Jaringan pada Server 4

2.2 Tidak diperlukan Akses Jaringan pada Server 5

3 Saran pada Server yang di Publikasikan ke Internet 5

3.1 Jangan Konfigur DNAT dalam NGAF 5

3.2 Konfigurasi DNAT dalam NGAF 6

BAB 3 Harap diperhatikan 6

BAB 1 Skenario

Application control policy mengkontrol paket data berdasarkan definisi TCP/IP dari interaksi paket data atau karakteristik dari layer aplikasi (dari OSI layer) untuk mencegah paket data yang tidak sah saat pertukaran data.

Departermen R&D dari perusahaan pengembang piranti lunak memiliki kontrol ketat terhadap penguna intranet dan perlu melarang akses Facebook selama jam kerja. Selain itu, untuk memastikan keamanan informasi, pengguna dilarang menggunakan Gmail untuk mengirim file, dan IAM dapat digunakan untuk mengatur kebiasaan pengguna.

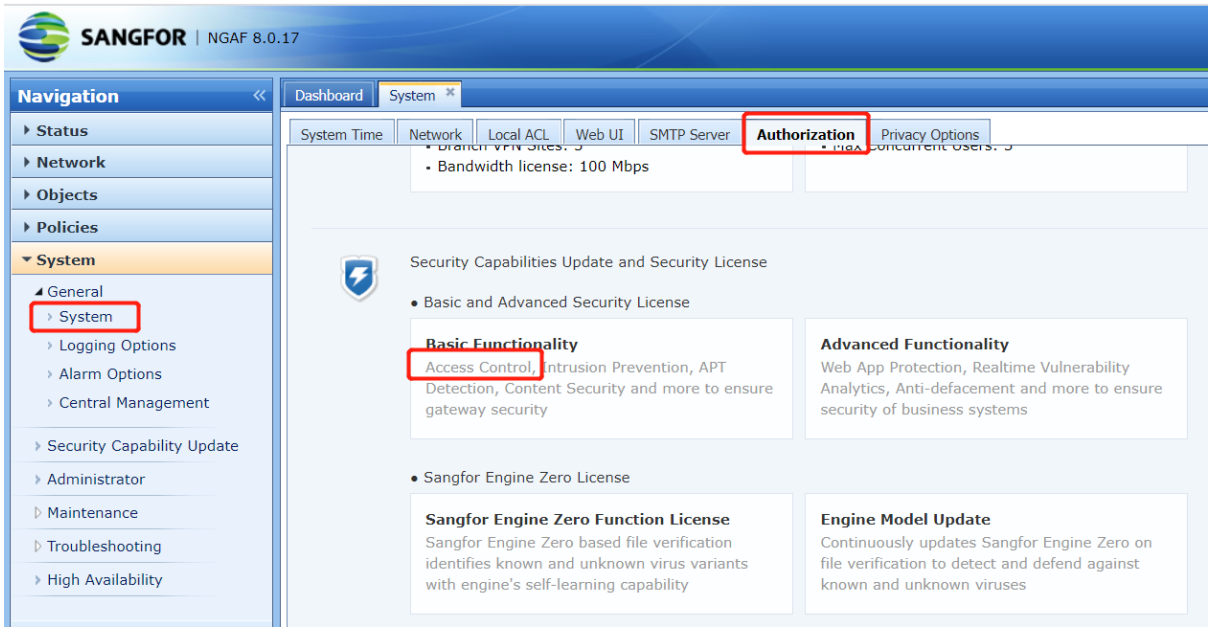
BAB 2 Pedoman Dasar

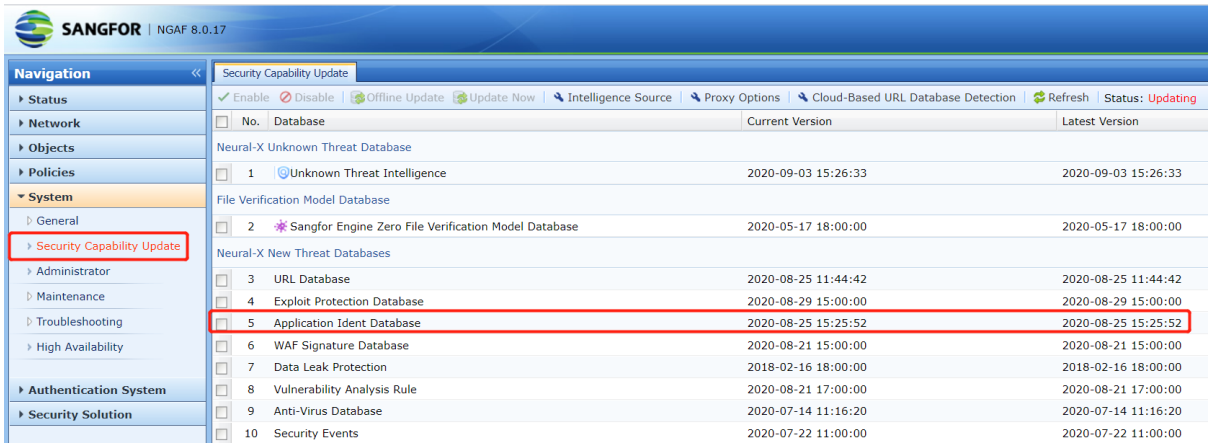
Dengan menerapkan application control policies, interaksi data dari kedua pihak dalam menentukan dan kendali dalam meminimalkan ijin akses, sehingga dapat mengurangi resiko keamanan dan serangan. saran ini hanyalah referensi saja. semuanya tergantung pada keadana khusus dan kondisi/perangkat aktualnya.

Catatan: Application control policy memotong semua interaksi yang mencurigakan pada umumnya. tetapkan paling tidak satu kebijakan untuk memastikan akses jaringan normal.

Pengecekan

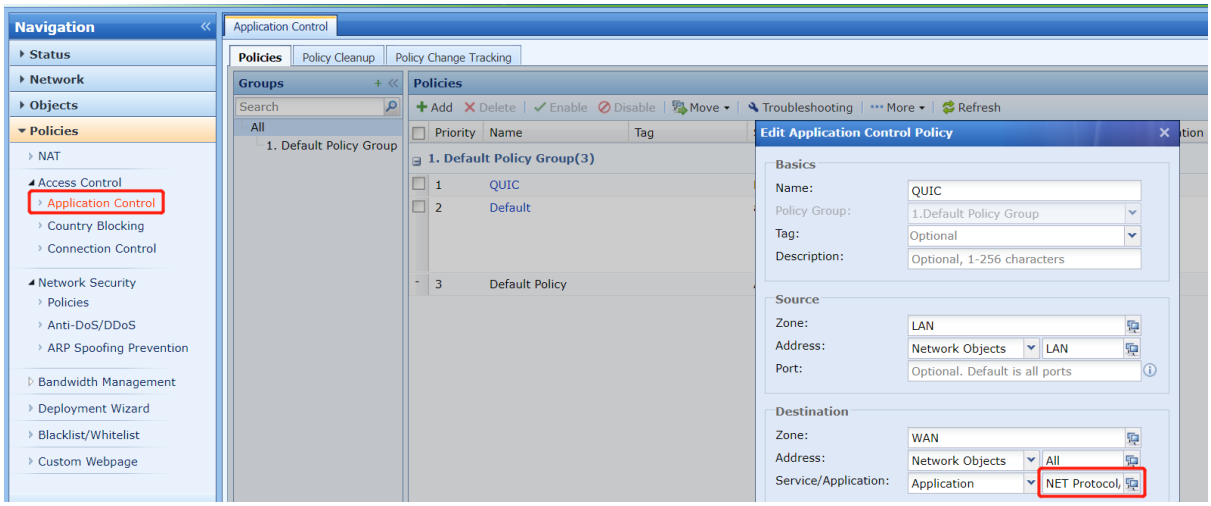
Periksa versi otorisasi dan database untuk memastikan telah diperbarui ke tanggal terbaru. Kebijakan application control policy untuk memproses paket data tergantung pada database. Jika database tidak diperbaharui ke versi terbaru, beberapa identifikasi trafik ada kemungkinan akan salah.





Blok Aplikasi Teracak/dienkripsi

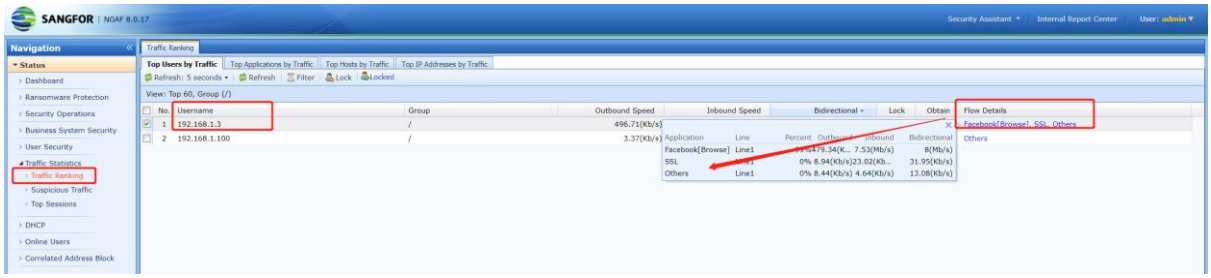
Saat ini banyak situs dan perambah/browser menggunakan protokol QUIC untuk mengirikan data, dan data yang dienkripsi oleh protokol QUIC tidak dapat dikontrol, sehingga protokol QUIC perlu dinonaktifkan. Setelah dinonaktifkan protokol QUIC, situs dan perambah akan secara otomatis menegosiasikan pengunaan HTTPS untuk transaksi data.



Jika anda ingin melakukan kontrol yang lebih mendetail pada prilaku menyimpang dari situs https, seperti mengijinkan browsing tetapi tidak diperbolehkan melakukan unggah lampiran. Anda perlu memeriksa deskripsi aturan NGAF untuk menentukan apakah anda perlu mengacak trafik yang relevan untuk nama domain. Contohnya, setelah melakukan query/permintaan penyaringan dari pengaturan, anda dapat mengetahui kalau pengunggahan lampiran ke Gmail perlu mengaktifkan dekripsi data SSL.

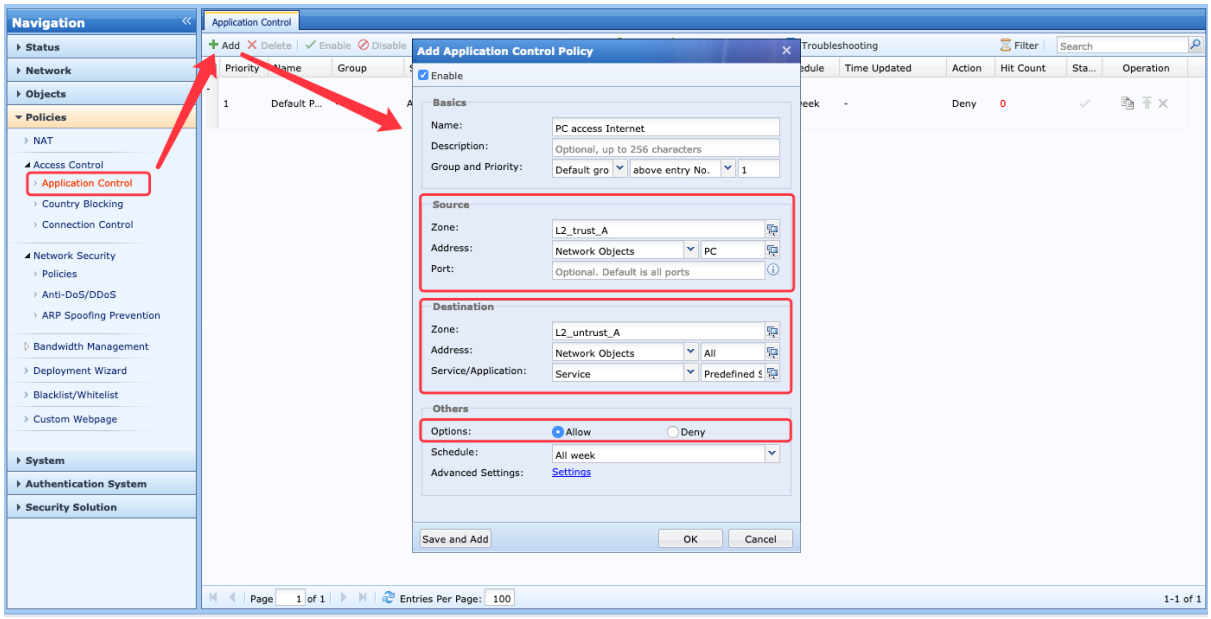
Pada beberapa aplikasi, beberapa aturan mungkin disertakan, sebagai saran untuk melakukan pemeriksaan aturan mana yang trafik sebenarnya dikenal oleh NGAF selama

pengujian. Kemudian pilih aturan yang tepat untuk memblokir aplikasi tersebut.



1 Saran Akses Jaringan pada PC

Untuk pengguna yang tidak memiliki hak kontrol PC untuk mengakses jaringan, disarangkan untuk menetapkan segmen dan Zona IP untuk PC, dan mengijinkan akses jaringan (dari LAN ke WAN) untuk semua aplikasi yang ada di PC. Konfigurasi sebagai berikut:

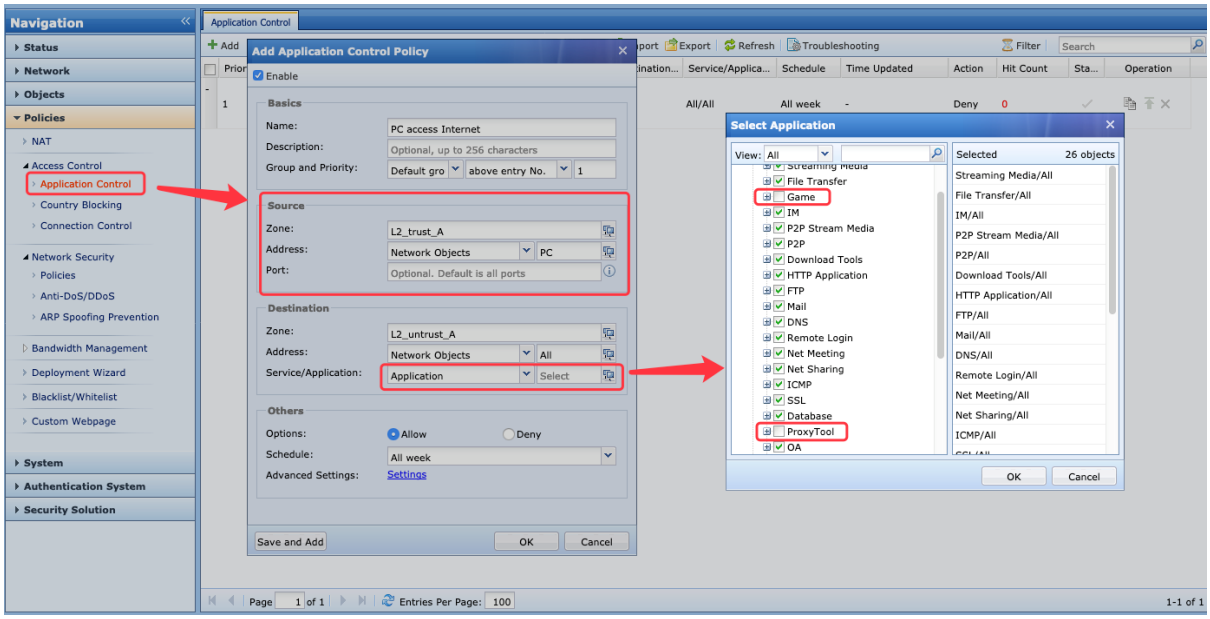


Catatan: Kebanyakan administrator lebih suka mengunakan satu policy untuk memperbolehkan semua IP untuk melakukan akses dua arah. Pedoman ini tidak direkomendasikan. Hanya cukup untuk memperbolehkan data akses dari LAN ke WAN jika tidak ada kebutuhan khusus pada PC tersebut.

Note: Perlu diperhatikan pada skenario ini: NGAF mengunakan bridge mode atau virtual wire mode, dan pengguna memiliki DHCP server pada WAN diluar dari AF (Contoh, set DHCP untuk gerbang terkoneksi ke AF). Pada skenario ini, diperlukan untuk memperbolehkan layanan DHCP dari WAN ke LAN: UDP port 67 dan 68, untuk memastikan PC terkoneksi dan dapat alamat IP dari DHCP.

1.1 Dengan Kebutuhan Kontrol khusus

Untuk PC pengguna yang memiliki kebutuhan khusus untuk mengakses jaringan (contoh, PC dapat mengakses jaringan, tetapi tidak dapat bermain game online ataupun mengunakan proxy luar). Dengan konfigurasi sebagai berikut.



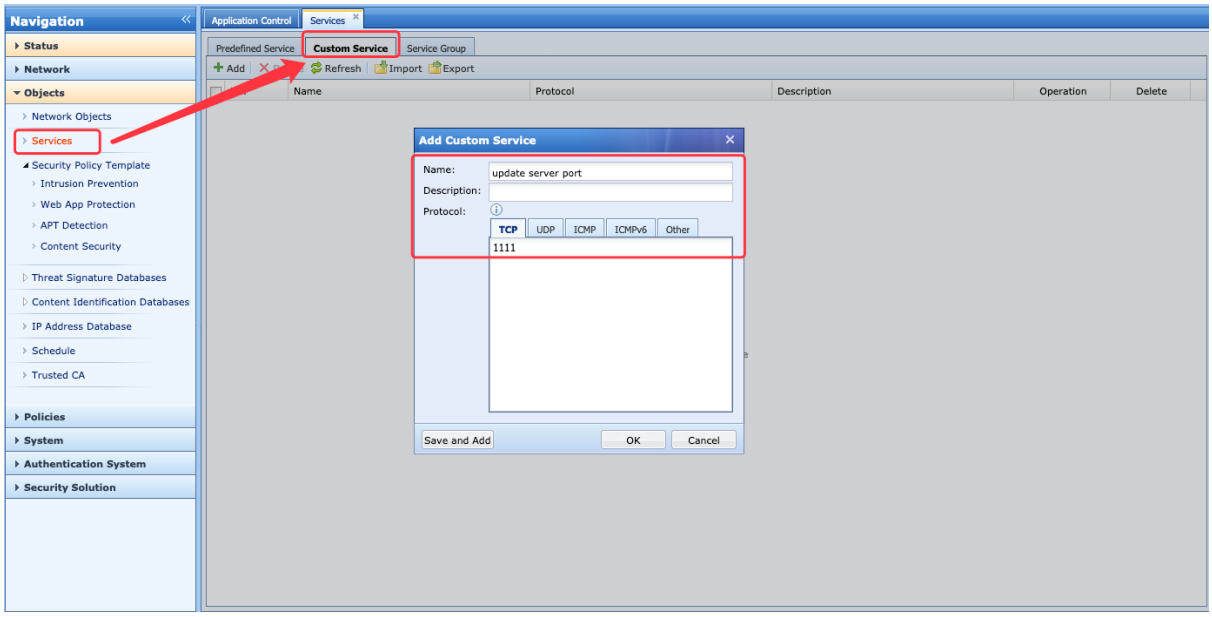
Catatan: Pada “Service/Application” terdapat tombol opsi, dan pilih spesifikasi tergantung dari kebutuhan. Jika tujuan port secara spesifik tidak diperbolehkan akses melalui WAN, akan lebih baik pilih “Service”

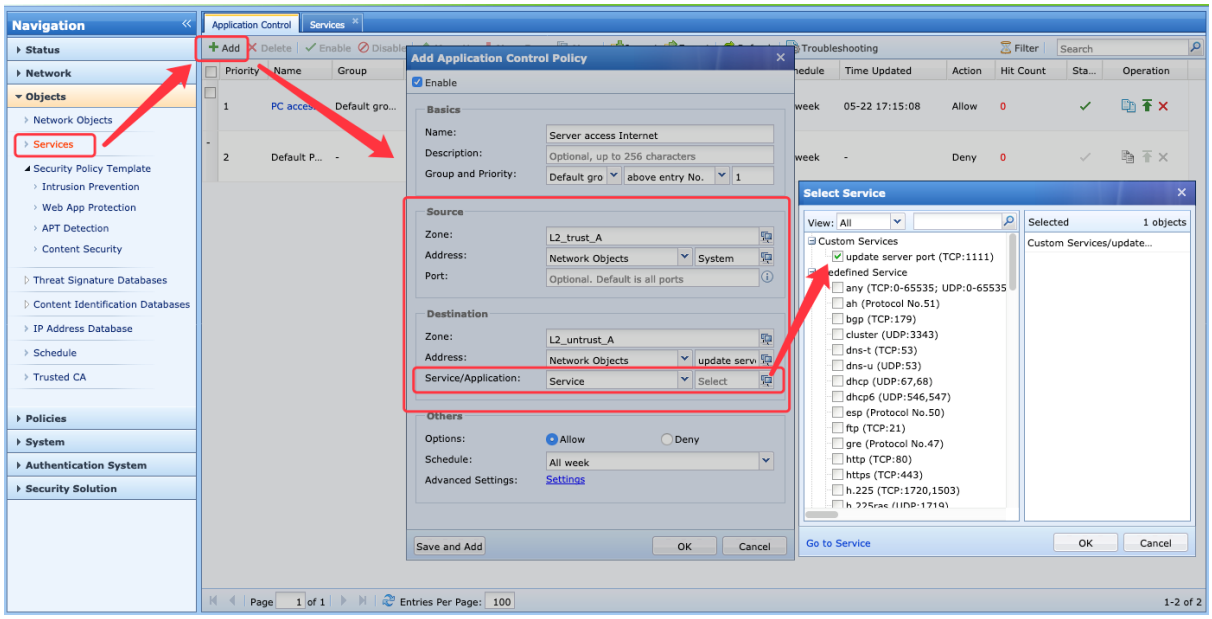
2 Saran Akses Jaringan pada Server

2.1 Kebutuhan Akses Jaringan pada Server

Pada umumnya kejadian ketika server perlu mengakses sumber tertentu secara khusus, seperti secara berkala melakukan pembaruan program atau sinkronisasi data ke server lain. Pada situasi seperti ini, direkomendasikan untuk menanyakan tujuan IP yang diakses ataupun port dari tujuan IP tersebut.

Contoh, Server situs portal memerlukan akses sinkronisasi ke server lain (200.200.200.200:1111) pada awan publik untuk melakukan push sinkronisasi data secara berkala.





2.2 Tidak diperlukan Akses Jaringan pada Server

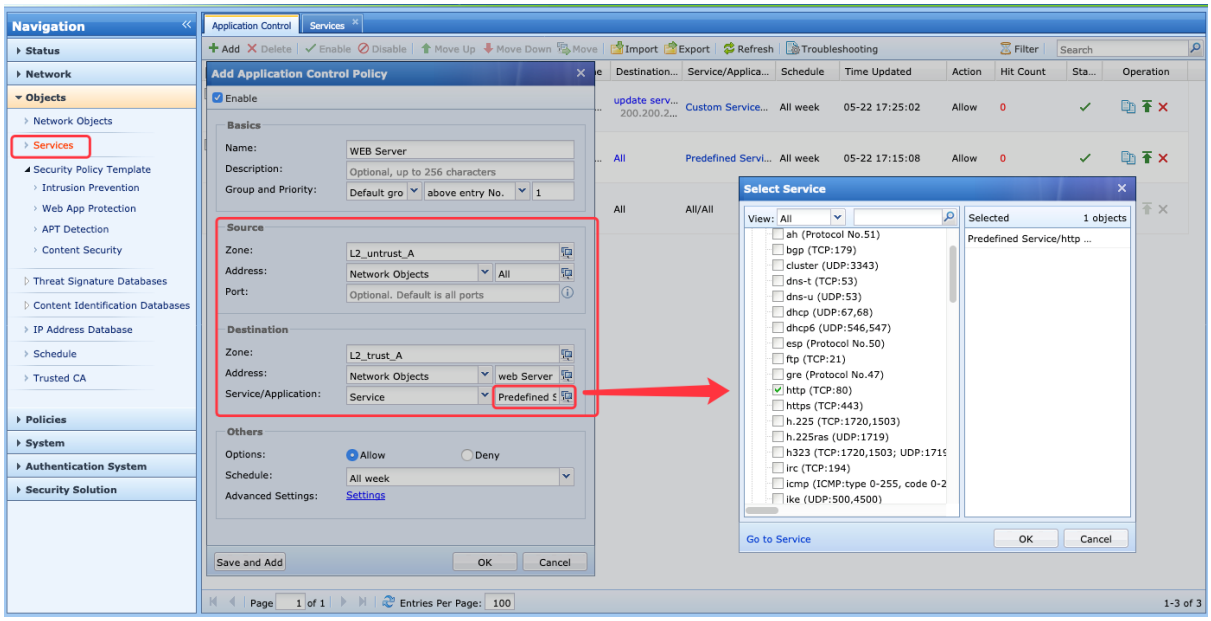
Pada kondisi ini, tidak diperlukan untuk mengkonfigurasi “Allow” policy apapun untuk tujuan dari server ke zone WAN. Umumnya policy akan diterapkan untuk mencegah akses jaringan yang menyimpang dari server.

3 Saran pada Server yang di Publikasikan ke Internet

3.1 Jangan Konfigur DNAT dalam NGAF

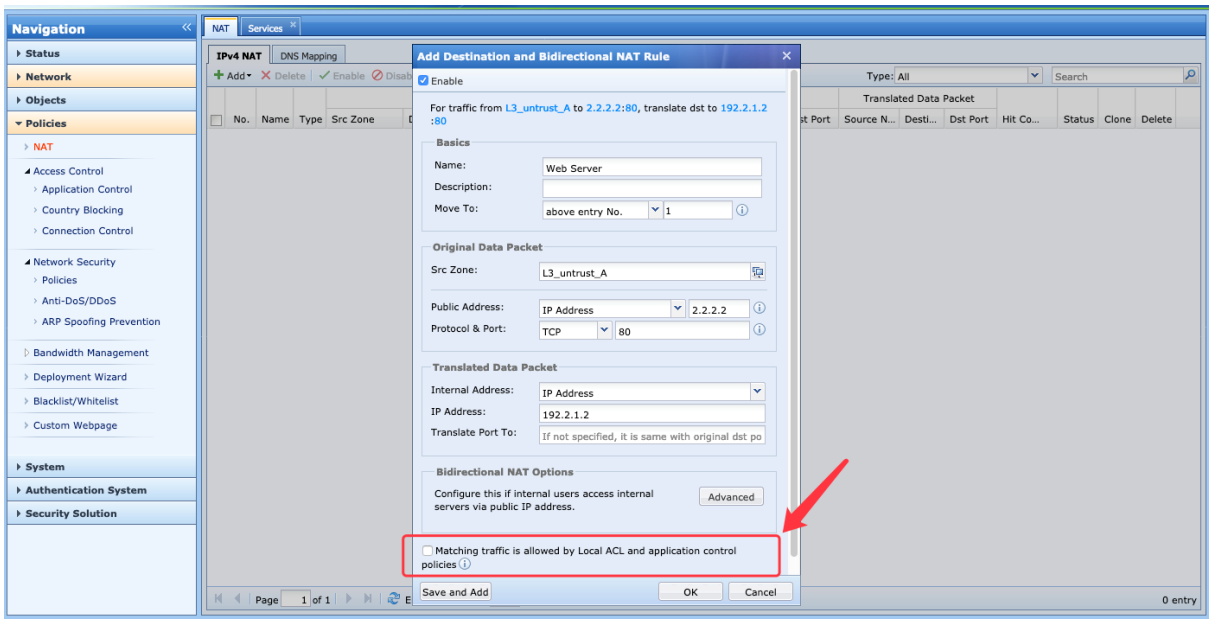
Pada skenario ini relatif sederhana. Server hanya perlu dipublikasikan port/layanan ke internet. port/layanan lainnya tidak diperbolehkan.

Contoh, Portal situs hanya memerlukan HTTP untuk dipublikasikan.



3.2 Konfigurasi DNAT dalam NGAF

Pada skenario ini, catatan bahwa dalam policy DNAT, Semua konten dari DNAT diperbolehkan untuk diakses dengan application control policy secara umum. Ketika dalam sebuah lingkungan dari full mapping untuk IP jaringan publik, direkomendasikan untuk diskusi dengan penguna dan melepaskan centrang pada opsi ini, dan secara manual aktifkan layanan dari application control policy.



BAB 3 Harap diperhatikan

- Hati-hati saat mengaktifkan “Persistent Connection” dalam [Application Control] – [Advanced Setting]. Hanya diaktifkan untuk server tertentu dengan persyaratan (jika diperlukan). Hindari terlalu banyak server yang diaktifkan untuk menghindari

lambatnya pelepasan tautan dari perangkat, yang akan mempengaruhi kinerja perangkat.

- Hati-hati saat mengaktifkan “Logging” dalam [Application Control] – [Advanced Settings]. Saran untuk menyimpan log kedalam “External Data Center” jika jumlah dari item yang akan dicatat sangat besar, untuk menghindari terlalu banyaknya log yang muncul dalam Interna Data Center pada umumnya, ini dapat berpengaruh pada performansi dari alat.

- [ApplicationControl] – [Troubleshooting] termasuk tiga fungsi didalamnya: “Policy Validity Check”, “Policy Troubleshooting” dan “Group Management”. Anda boleh memperkenalkan fungsi ini kepada pengguna untuk menjelaskan fitur dari produk secara sederhaana dan mudah untuk digunakan.