SANGFOR

NGAF

Pedoman terbaik untuk Skenario Botnet Prevention

Versi 8.0.17

Data Perubahan

Tanggal	Keterangan Perubahan
June 15, 2020	Rilis Dokumen
Mar 18, 2021	Pembaruan Dokumen
May 17, 2021	Pembaruan Dokumen

DAFTAR ISI

BAB 1 Skenario

1.1 Perkenalan Fungsi

Piranti anti-virus dan firewall pada umumnya memiliki keterbatasan efektifitas dalam menditeksi trojan. Pada skenario APT (Advanced Persistent Threat), Antivirus dan Firewall biasa memiliki tingkat diteksi dan pertahanan yang lemah. Oleh sebab itu, sistem penditeksian secara dini diperlukan untuk menditeksi dan mengenali mesin yang terinfeksi untuk memperkecil resiko yang terjadi pada komputer pengguna. Pada saat yang sama, sejarah dari data perubahan sangat penting untuk melakukan penelusuran.

1.2 Pengujian URL

Anda dapat menguji melalui URL berikut:

ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com

iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

v.beahh.com

aqhln.ws

mlmy.3322.org

www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

clptiiybpip.cn

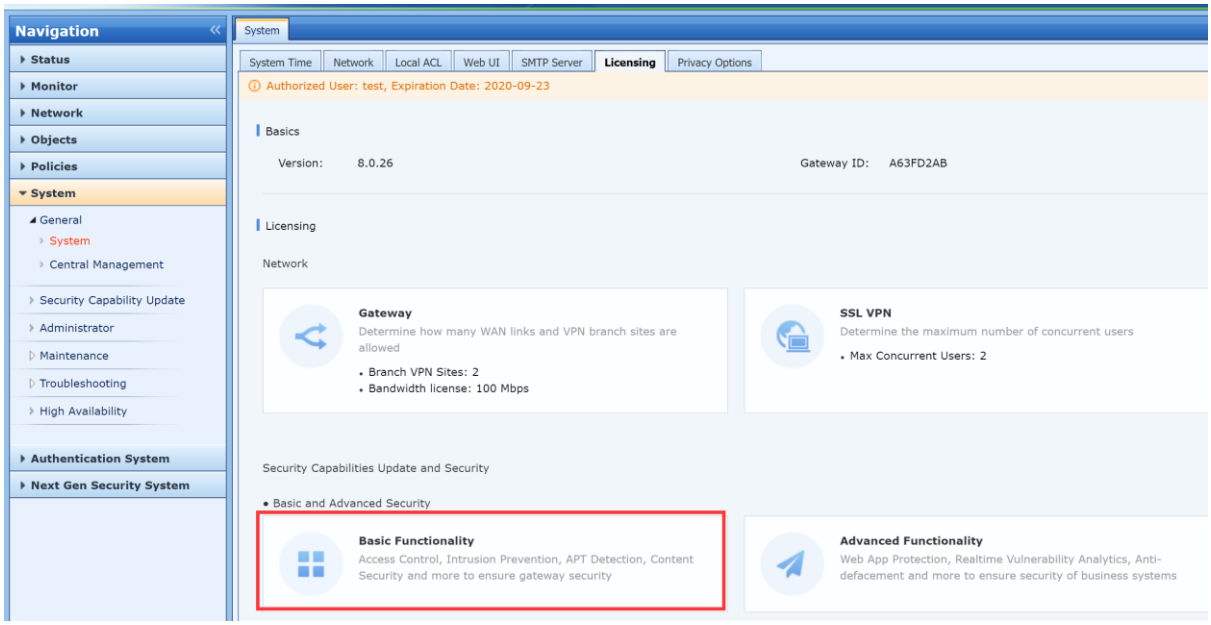
task.attendecr.com

bddp.net

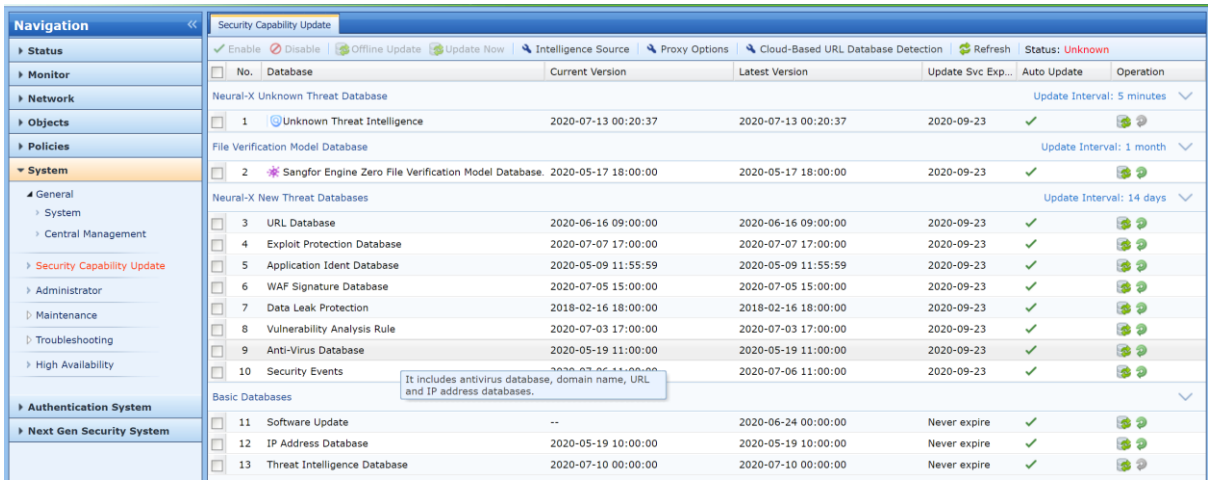
cqogflioz.cn

BAB 2 Pedoman yang disarankan

Lakukan pengecekan lisensi untuk memastikan Fungsi lisensi telah diaktifkan pada perangkat.

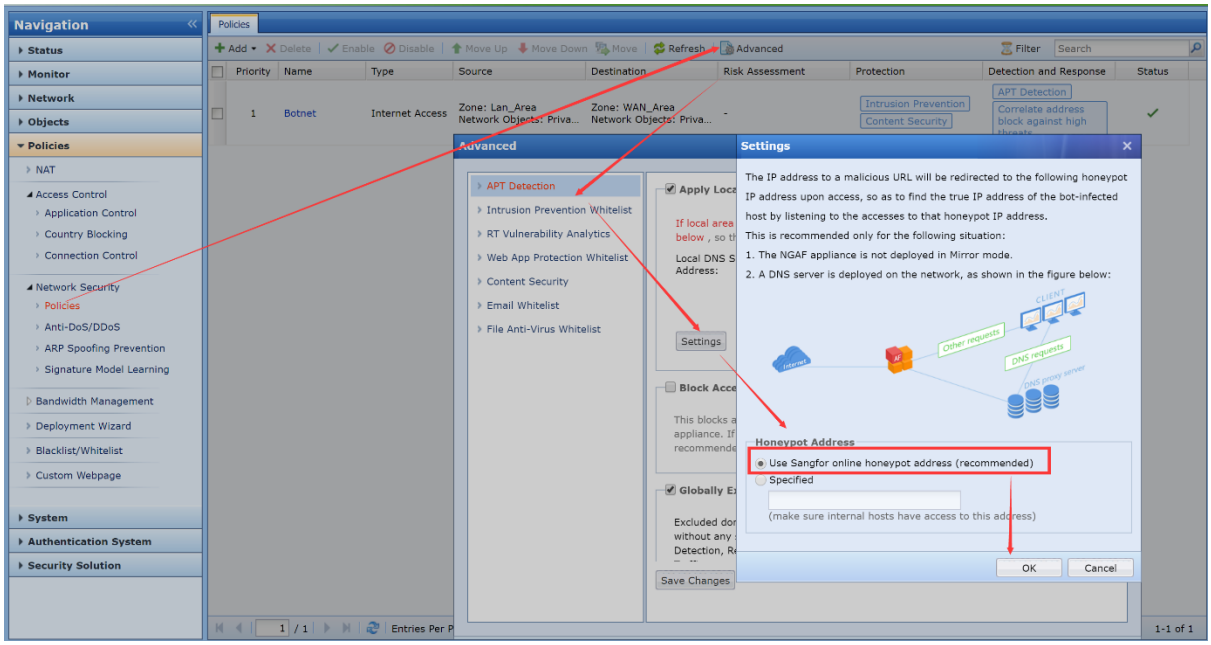


Pastikan database telah diperbarui hingga pembaruan terbaru.



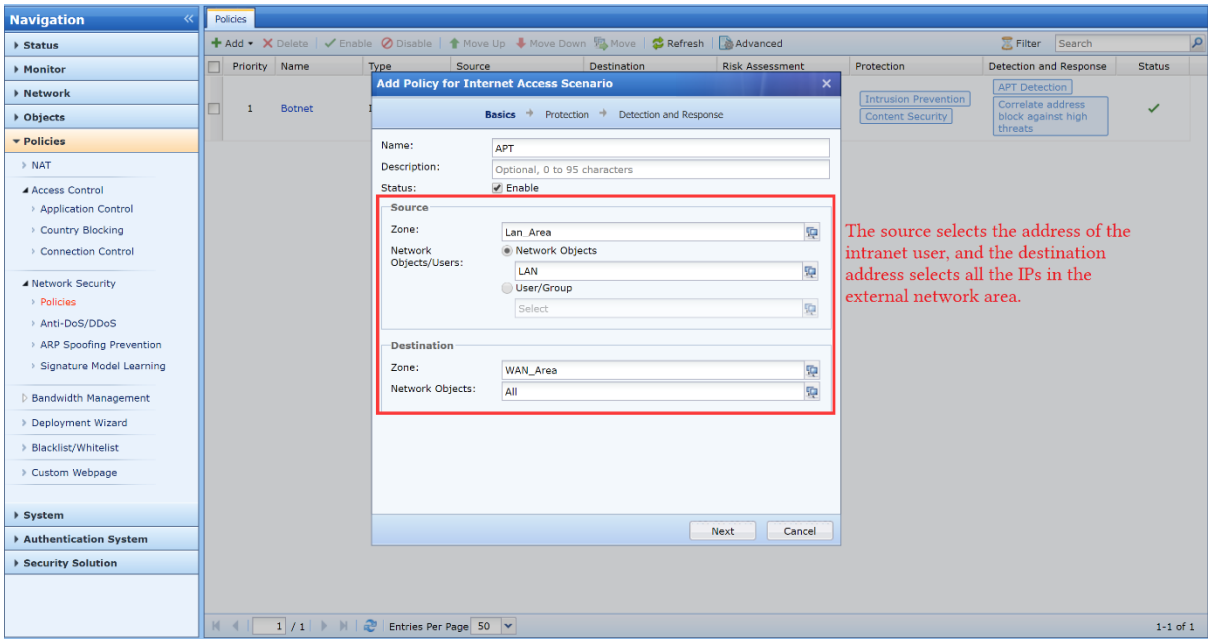
Proteksi Botnet direkomendasikan untuk server dan workstation, keduanya memiliki resiko terinfeksi yang sama.

Catatan Penting: Jika memiliki DNS server dalam intranet dan pengguna intranet mengunakan DNS dari intranet untuk nama domain yang digunakan, “Honeypot” adalah teknelogi yang harus di aktifkan. Meneruskan permintaan DNS dengan cara sebagai berikut dibawah ini:

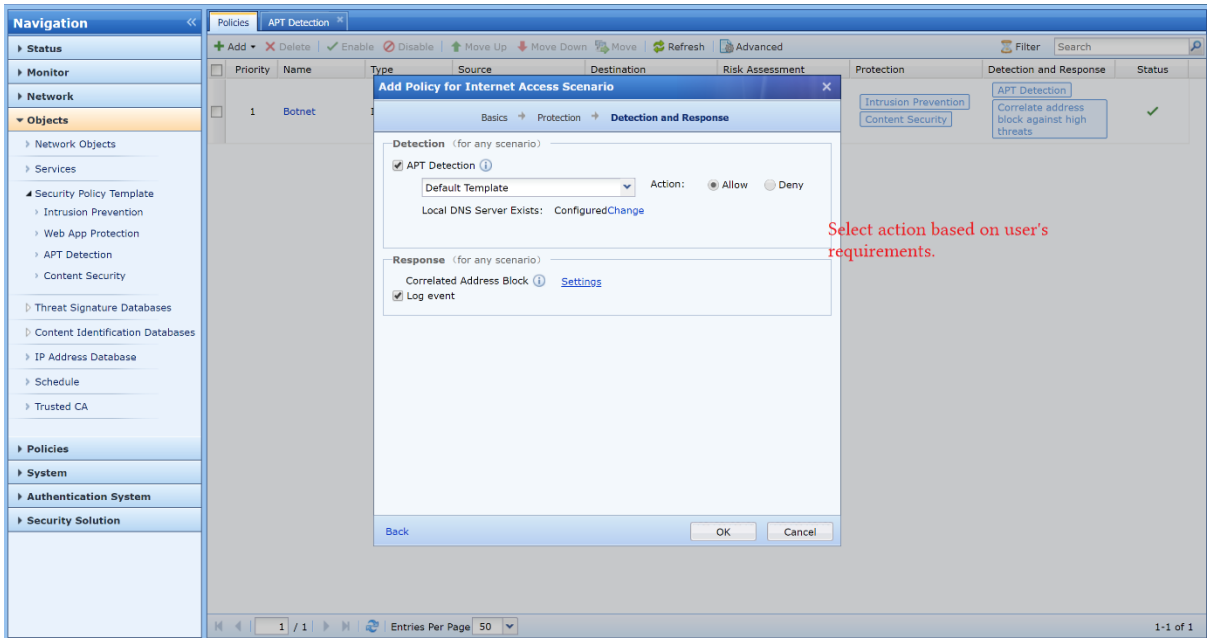


2.1 Rekomendasi Policy Proteksi pada Endpoint

Tambahkan area dan policy, Proteksi Enpoint dibutuhkan memilih arahan untuk memperhatiakan area asal adalah area internal jaringan, area tujuan adalah area jaringan publik.

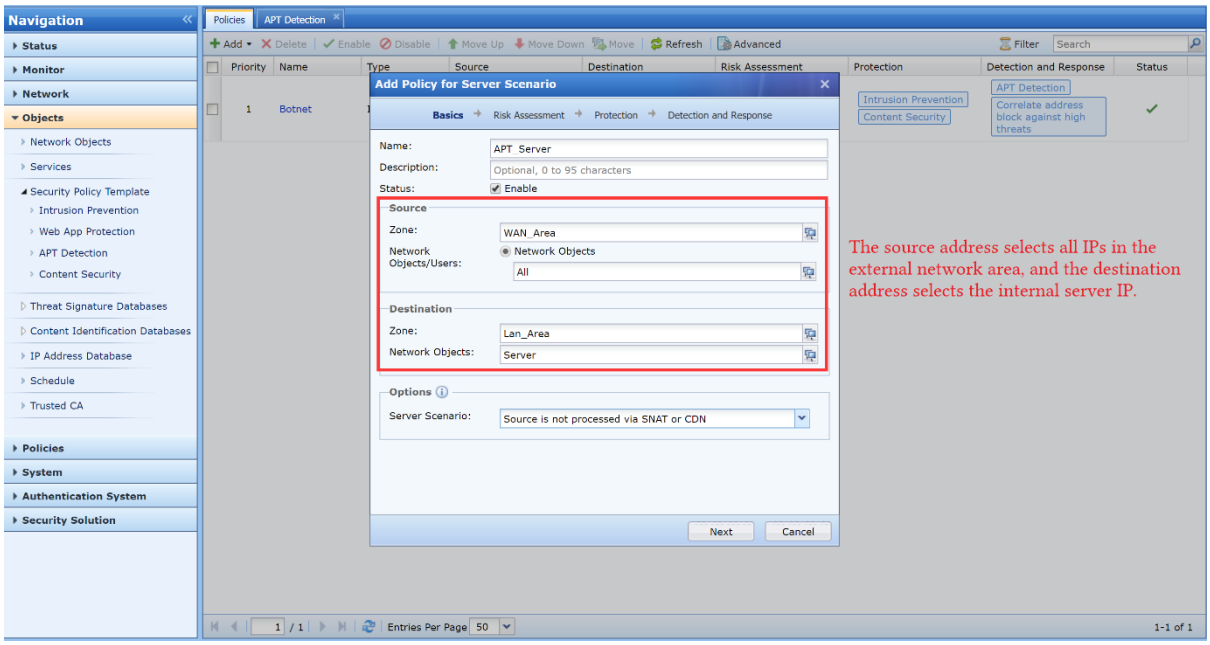


Untuk mengaktifkan fungsi botnet, gunakan “Default template” untuk policinya dan “Deny” untuk aksi sebagai kebutuhan melakukan pertahanan yang dibutuhkan.

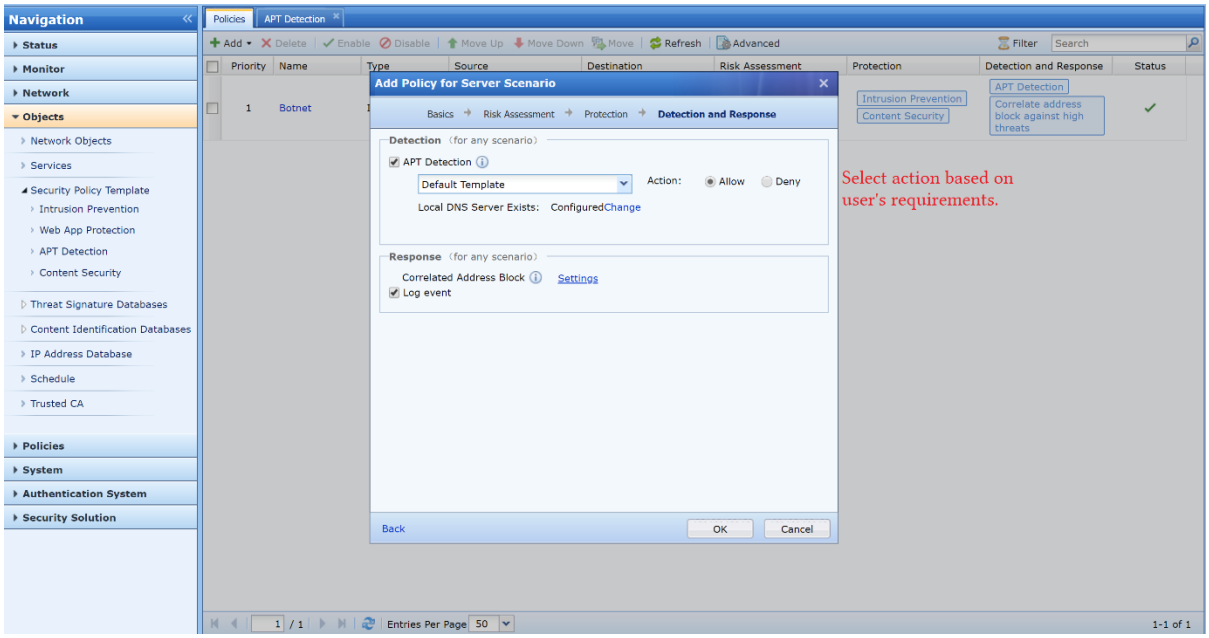


2.2 Rekomendasi Policy Proteksi pada Server

Tambahkan policy dan pilih area yang diperlu diproteksti. Proteksi Server dibutuhkan memilih arahan untuk memperhatiakan area asal adalah area internal jaringan, area tujuan adalah area jaringan publik.



Untuk mengaktifkan fungsi botnet, gunakan “Default template” untuk policynya dan “Deny” untuk aksi sebagai kebutuhan melakukan pertahanan yang dibutuhkan.



Chapter 3 Perhatian

Aksi dari policy botnet, Skenario akses untuk "Policy for Server Scenario" atau "Policy for Internet Access Scenario ", pada dasarnya adalah “allow”, jika anda ingin meruhannya menjadi “Deny”, anda perlu memilihnya secara manual;

Fungsi botnet dalam "Policy for Internet Access Scenario" dapat secara otomatis tersedia pada area yang telah dipilih melalui policy. Contohnya, area yang dipilih dalam "Policy for Internet Access Scenario" adalah semua external network area, dan tujuan area adalah internal network area. Tujuannya untuk mengidentifikasi dan prosess dari botnet, sumber adalah internal network area dan yang menjadi target adalah external network area;

Fungsi “Suspicious Trafik” dari botnet tidak melakukan blok terhadap perlakuan yang tidak biasa, ia hanya melakukan diteksi, dan hanya menyalinnya dalam log dan pada saat yang sama pencatatan paket data original untuk nantinya dilakukan penelusuran.