SANGFOR

IAG

Panduan Konfigurasi Access Check/Control

Versi 13.0.15

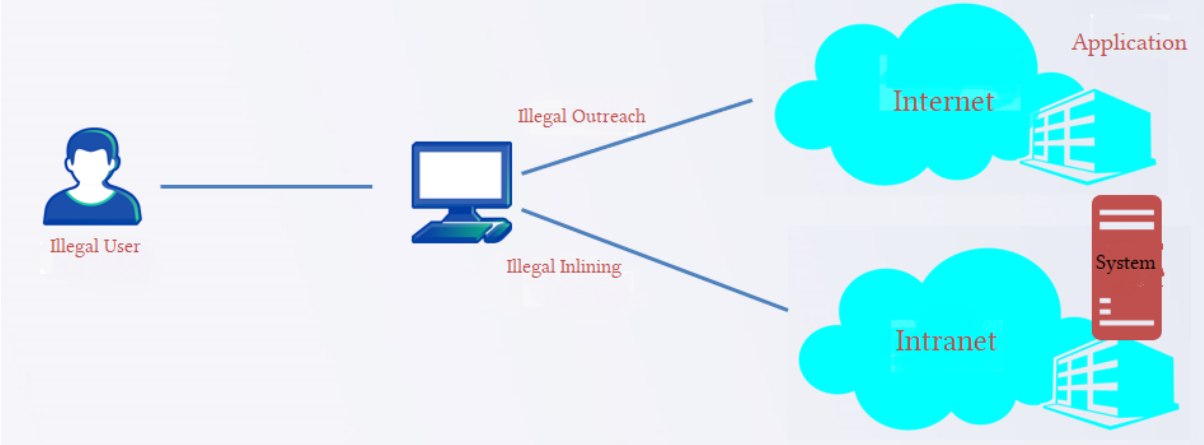
Catatan Perubahan

Tanggal	Deskripsi Perubahan
September 8, 2020	Rilis Dokumen Version 13.0.8.

Daftar Isi

Bab 1 Latar Belakang Permintaan

- Private network tidak mengizinkan terminal terhubung ke network lain untuk mencegah kebocoran data.
- Terminal memiliki outreach dan tindakan inline, dan illegal access tidak dapat dikontrol.



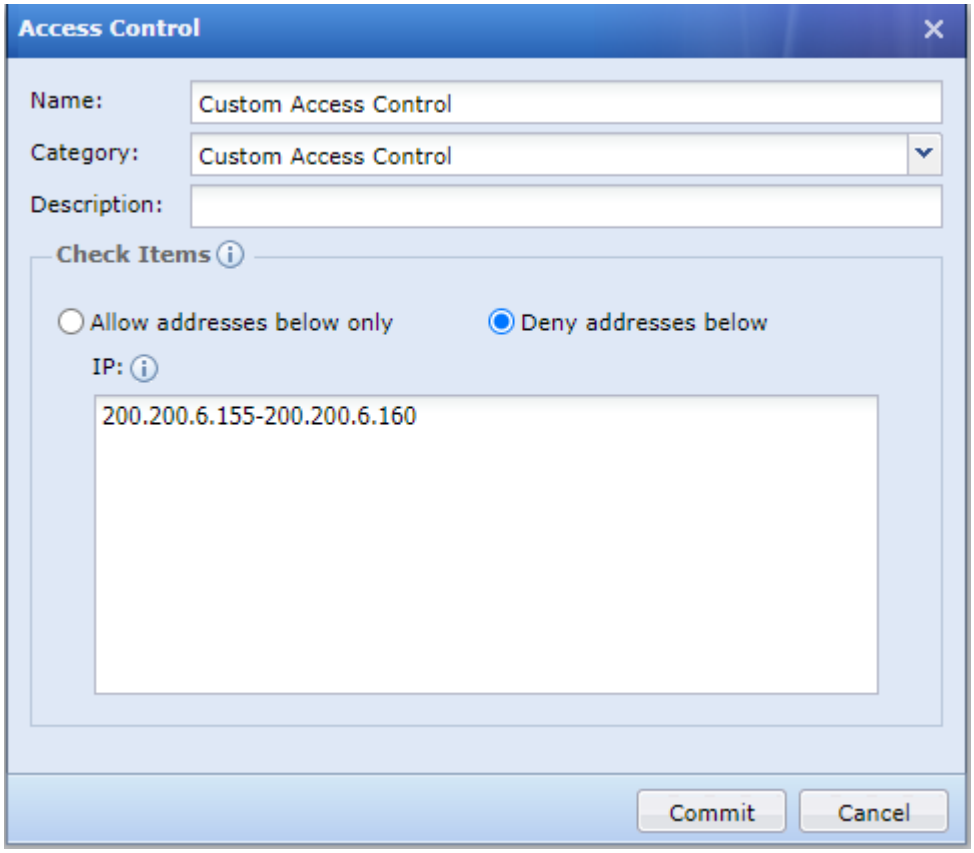
Bab 2 Penjelasan Fitur

2.1 Access Check

- Dialup: Menentukan perilaku dialup dengan memeriksa antarmuka API sistem atau fungsi, jika ada perilaku dialup, itu dianggap sebagai pelanggaran
- Network adapter terkait: Dengan mendeteksi antarmuka API terkait atau fungsi dan registry informasi terkait untuk mendeteksi apakah ada wireless network card, 4G network card dan perilaku dual network card, jika ada, anggap itu sebagai pelanggaran.
- External network: Periksa apakah website berikut dapat di-ping, jika dapat di-ping, anggap dapat terhubung ke external network (www.taobao.com, www.jd.com, www.baidu.com, www.sangfor.com, www.ifeng.com, 5 website dikontrol oleh sistem backend konfigurasi file, yang dapat dimodifikasi melalui backend)
- WiFi Tidak Aman: Dapatkan informasi SSID dengan memeriksa antarmuka API sistem atau fungsi , kemudian bandingkan dengan SSID yang diatur dalam whitelist, jika SSID yang terhubung tidak ada dalam whitelist, anggap itu sebagai pelanggaran.
- Gateway Tidak Valid: Dapatkan semua fisik network cards dengan memeriksa antarmuka API sistem atau fungsi. Gateway network card dibandingkan dengan address yang diatur dalam whitelist, itu dianggap sebagai pelanggaran.
- Custom: IP/domain name dan port dapat diatur, memungkinkan ingress untuk mendeteksi apakah dapat diakses, jika dapat diakses dianggap sebagai pelanggaran. Ketika port kosong, defaultnya adalah port 80.

2.2 Access Control

- Memohon antarmuka Windows Sistem WFP (Windows Filtering Platform) API dalam framework untuk mencapai fungsi micro-isolation.
- PC Windows XP tidak mendukung manajemen dan control (XP tidak memiliki WFP framework).
- Mendukung black dan white list, Mendukung IP dan port, jika port kosong, port default adalah 1-65535.



Bab 3 Skenario Aplikasi

- Fungsi access check/control terutama digunakan dalam skenario private network, jika ditemukan bahwa terminal memiliki illegal access, seperti perilaku koneksi internet, itu diblokir dengan melarang terminal network card.

- Control terminal access izin melalui black dan white list, seperti hanya mengizinkan access ke IP tertentu atau melarang access ke IP range tertentu.

Bab 4 Konfigurasi

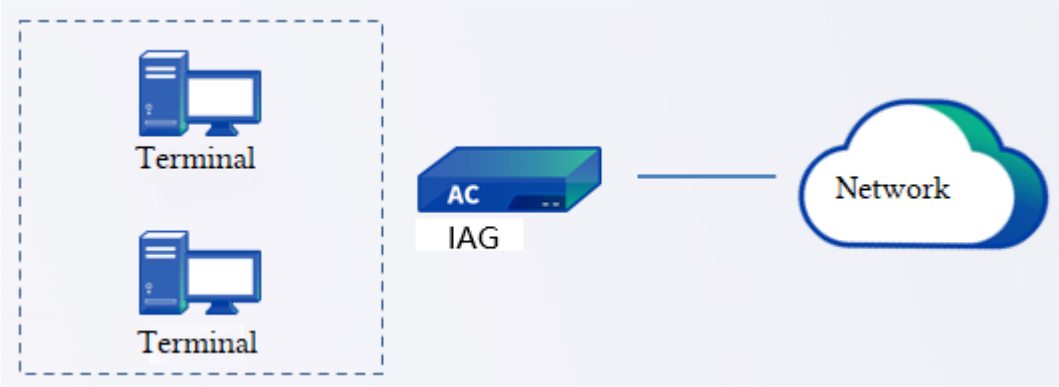
4.1 Langkah Konfigurasi:

1. Buat baru access check/control rule dan konfigurasi spesifik inspeksi item atau control item .

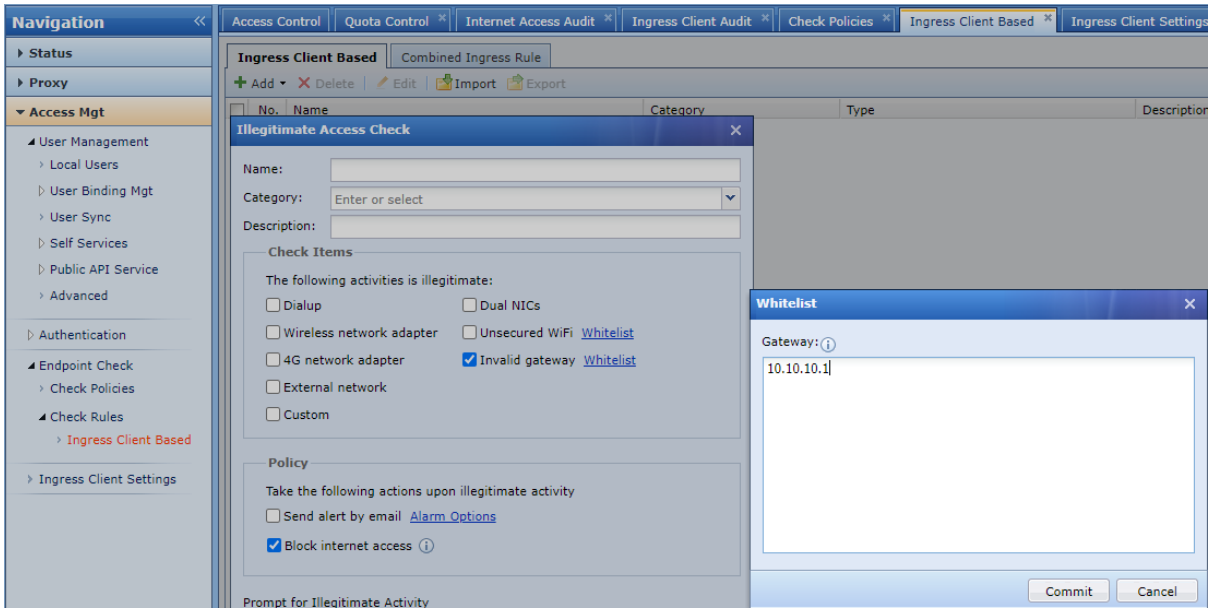
2. Konfigurasi endpoint check policy, lihat ke aturan yang dikonfigurasi sebelumnya, dan pilih pengguna yang dapat diterapkan.

4.2 Kasus Konfigurasi:

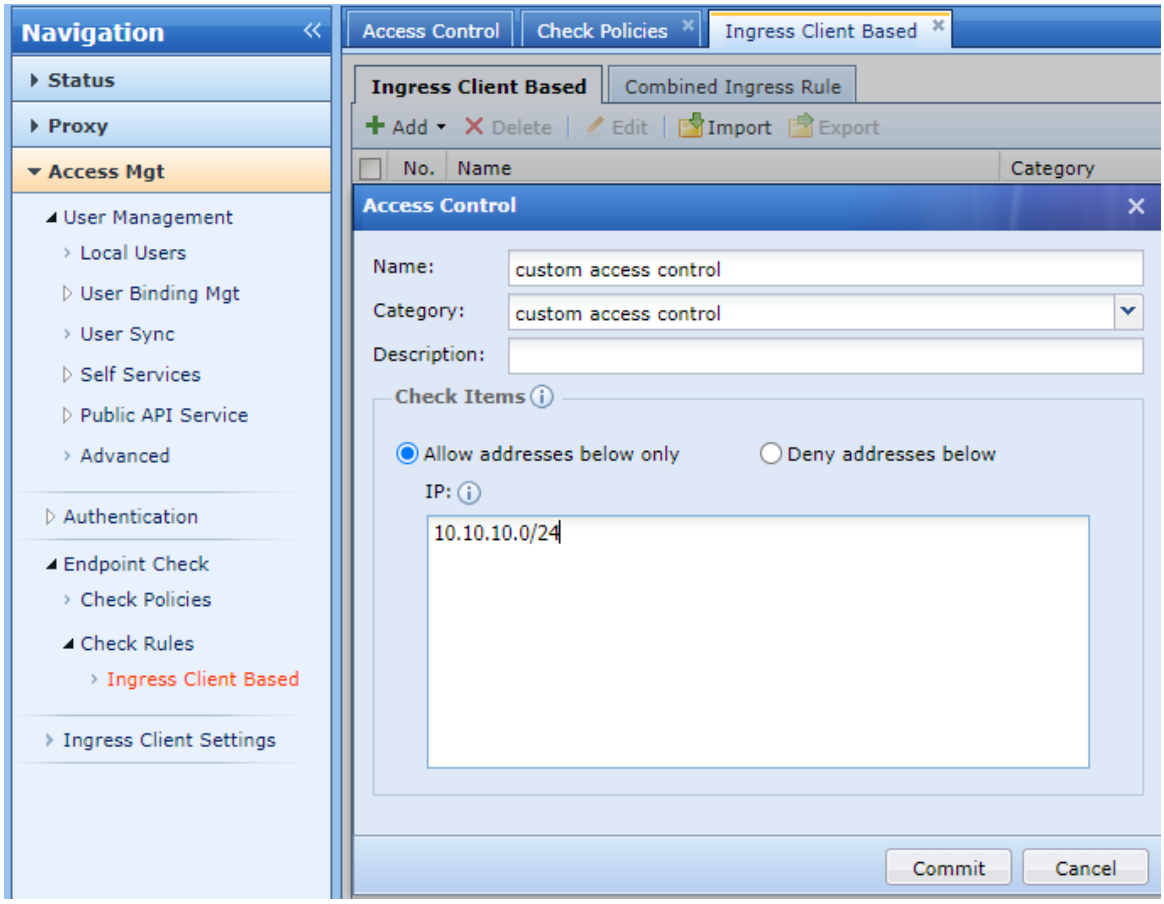
Customer memasang IAG pada private network mereka. Gateway dari terminal wajib menjadi 10.10.10.1. Ketika ada gateway lainnya, network akan terputus. Address segmen yang dapat diakses pada saat yang sama hanya dari 10.10.10.0/24.



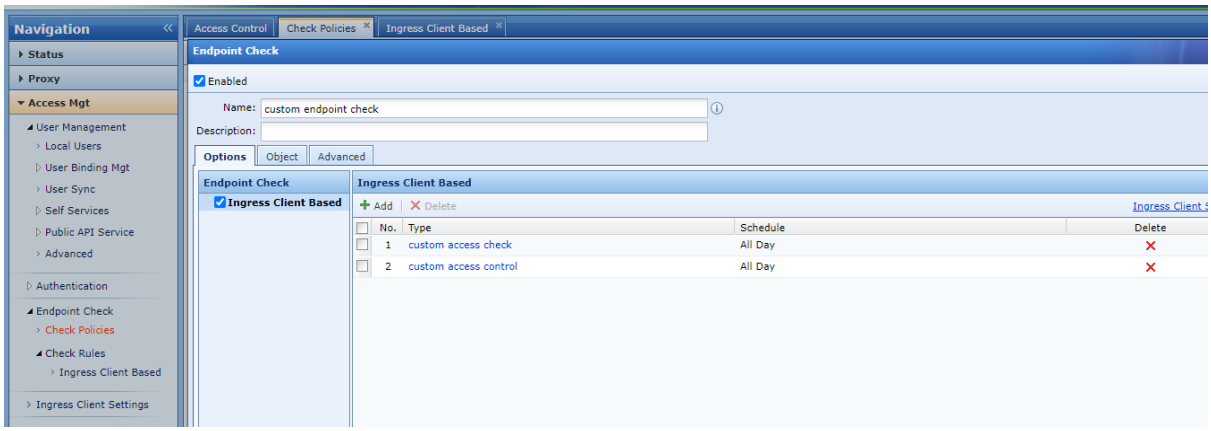
Buat baru access check rule, centang invalid gateway, dan isi 10.10.10.1 di whitelist.



Buat baru access control rule, dan hanya mengizinkan access ke bagian 10.10.10.0/24.



Buat baru endpoint check policy, tambahkan access check dan control rule yang dibuat sebelumnya, dan pilih pengguna yang dapat diterapkan.



Bab 5 Tindakan Pencegahan

1. Terminal hanya dapat memperoleh policy setelah melewati autentikasi, dan ingress client harus diinstal untuk access check dan fungsi control.

2. Tidak boleh ada NAT di path dari terminal ke perangkat IAG. Jika ada NAT, access check dan fungsi control tidak akan berpengaruh.

3. Sistem XP tanpa WFP module tidak mendukung fungsi access control.

4. Gabungan ingress rule tidak menerapkan access check dan control rule (gabungan ingress rule adalah old ingress rule seperti proses dan file berbasis rule).

5. Ingress yang diinstal melalui MSI tidak dapat mencegah uninstalasi. Jika Anda ingin mencegah uninstalasi, Anda perlu menginstal ingress dalam format exe, dan aktifkan fungsi pencegahan uninstal dalam pengaturan ingress client, dan terminal perlu mendapatkan endpoint check policy. (Anda dapat mengunduh ingress dengan memunculkan halaman instalasi ingress dengan mengkonfigurasi endpoint check policy, atau Anda dapat mengunduh melalui http://IP:817/singress.exe langsung pada perangkat).

6. Ketika network terputus, semua physical network cards akan dinonaktifkan. Setelah diaktifkan kembali, akan ada 40 detik untuk mendeteksi apakah ada pelanggaran. Jika ada pelanggaran, network card akan kembali dinonaktifkan. Ketika tidak ada pelanggaran, network card tidak akan lagi diblok. Jika policy diperbaharui, itu juga akan diperbaharui dalam 40 detik.

SANGFOR