SANGFOR

Endpoint Secure

Praktik Terbaik untuk Skenario General Micro-Segmentation Policy

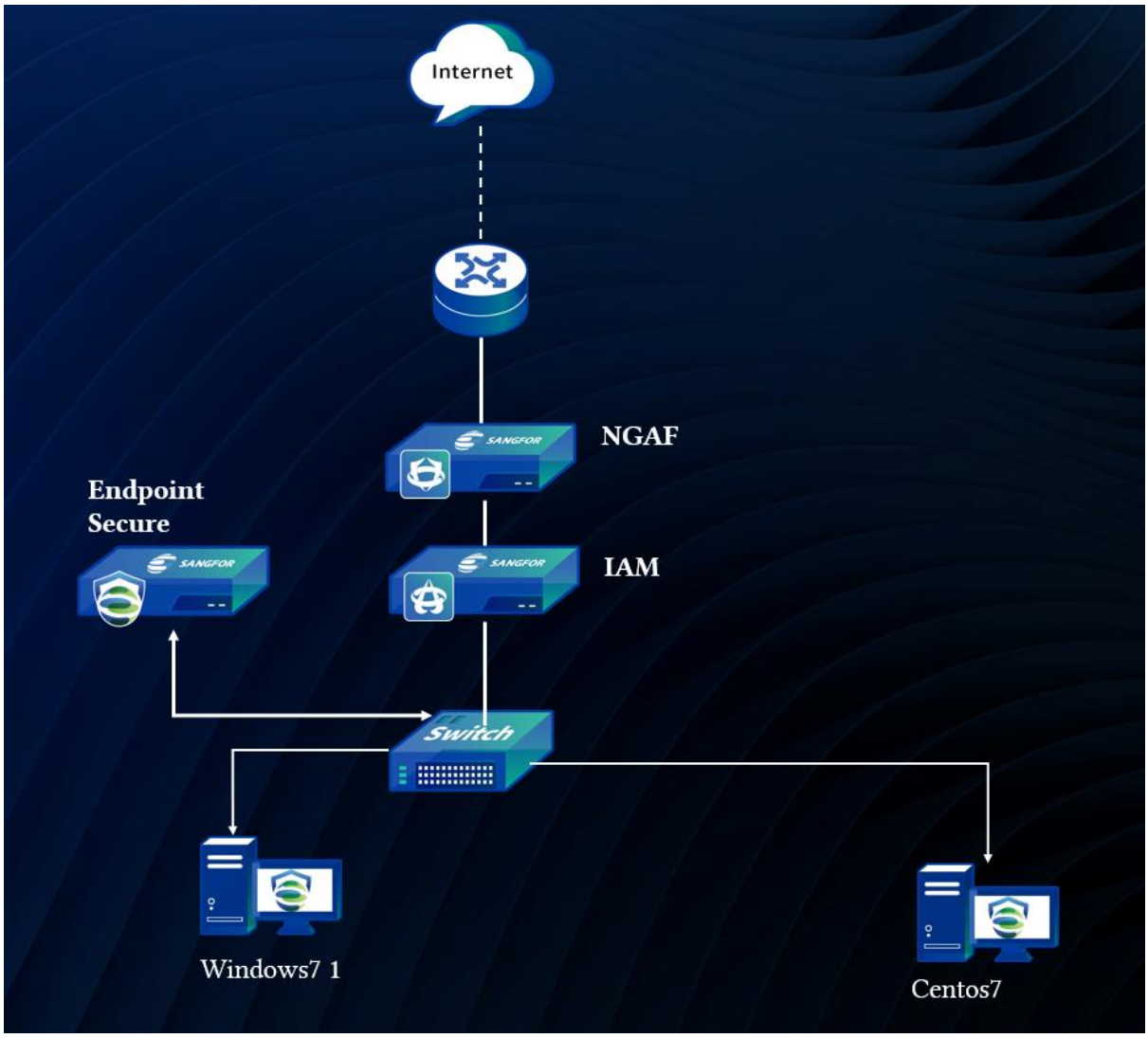
Catatan Perubahan

Tanggal	Deksripsi Perubahan
5 Janari 2020	Dokumen Terbit.
17 Mei 2021	Dokumen diperbarui.

CONTENT

Bab 1 Skenario

Dalam perusahaan ukuran kecil ataupun medium, ada zona DMZ di intranet untuk menyebarkan server untuk memberikan external web services, dan ada pengguna biasa mengakses internet di intranet. Sejak tidak adanya kebiasaan mengisolasi intranet, jadi pengguna intranet dapat mengakses server, ini dapat menempatkan server posisi beresiko, pada saat bersamaan, pengguna tidak dilarang untuk mengakses server. Karena itu diperlukan untuk melarang pengguna intranet mengakses port server yang beresiko tinggi untuk menghindari pengaksesan langsung pada port server yang beresiko tinggi oleh pengguna intranet.



Bab 2 Latar Belakang

2.1 Konsep WFP

Windows Filtering Platform (WFP) adalah basis framework untuk operasi interaktif pada paket data dalam lima layer dari stak protokol TCP/IP diluncurkan oleh windows. Framework memberikan API seri untuk tujuan interaksi. Role dari framework ini adalah untuk mengganti teknologi TDI/NDIS/LSP sebelumnya.

Menggunkan WFP API, developer dapat menerapkan personal firewall, intrusion detection system, program antivirus, dan alat pemantau traffic. WFP terintegrasi fungsi kontrol process-based firewall, tetapi ini tidak firewall itu sendiri, ini hanya development framework untuk packet filtering.

2.2 Untuk Endpoint Secure

Micro-segmentation policy dapat menargetkan empat macam objek dari: Business Systems, Tags, Servers, IP Groups

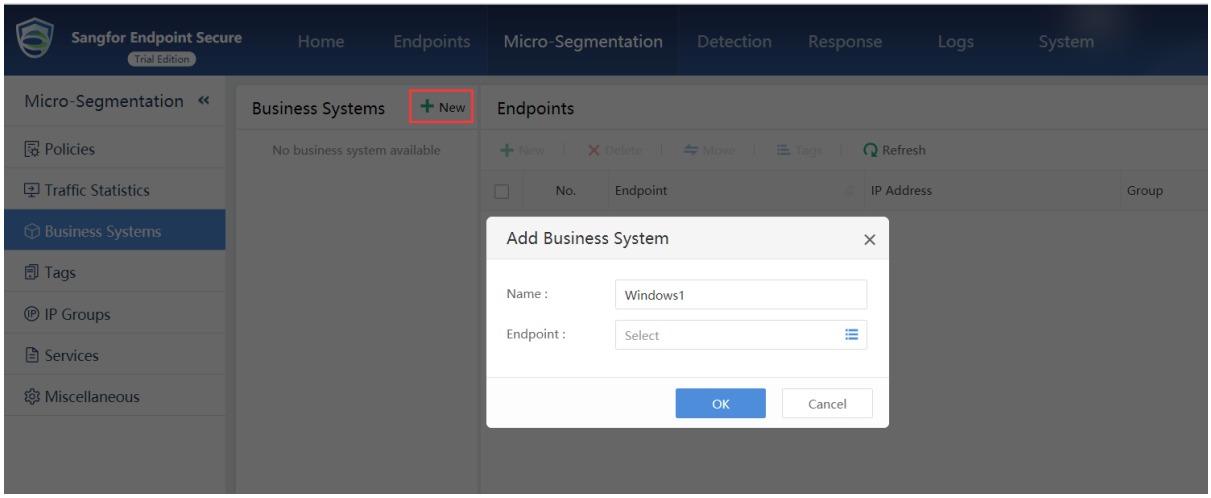
Kebutuhan Sistem Windows Vista, Windows 7, Windows 10

Windows Server 2008 dan versi selanjutnya.

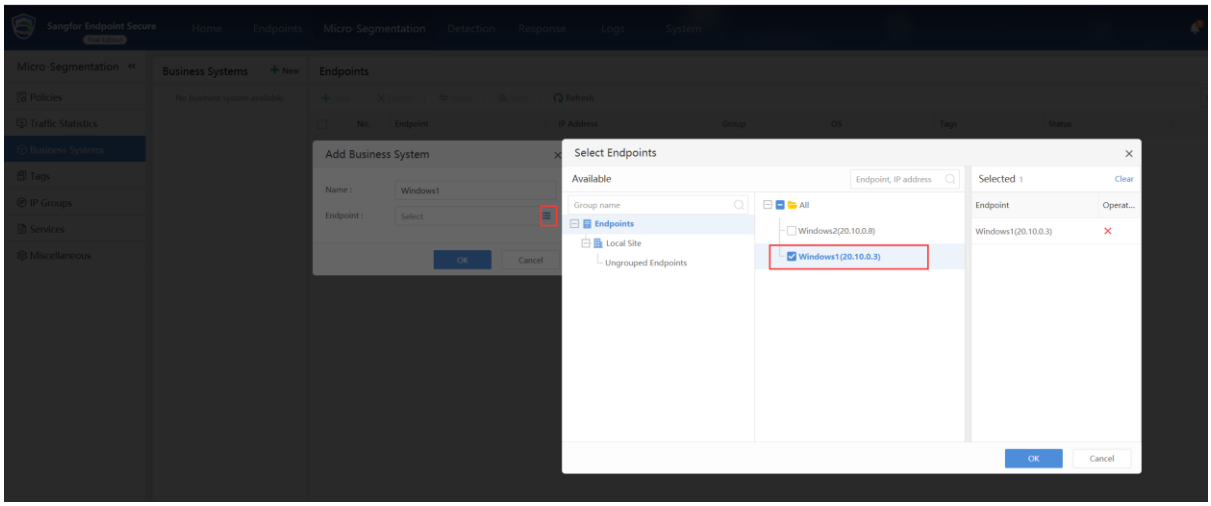
Bab 3 Konfigurasi

3.1 Tentukan Policy Object

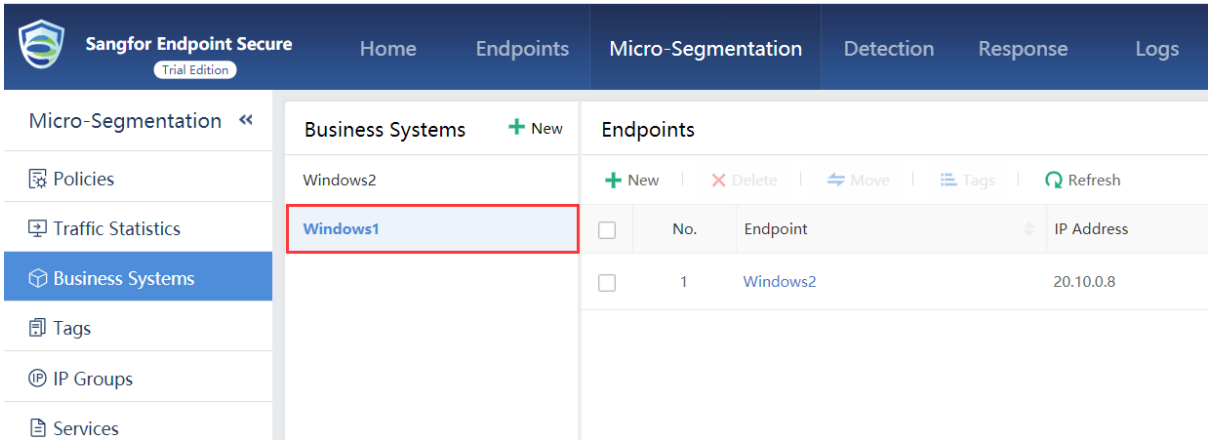
1.Tentukan Business System.



2.Pilih spesifik endpoint.

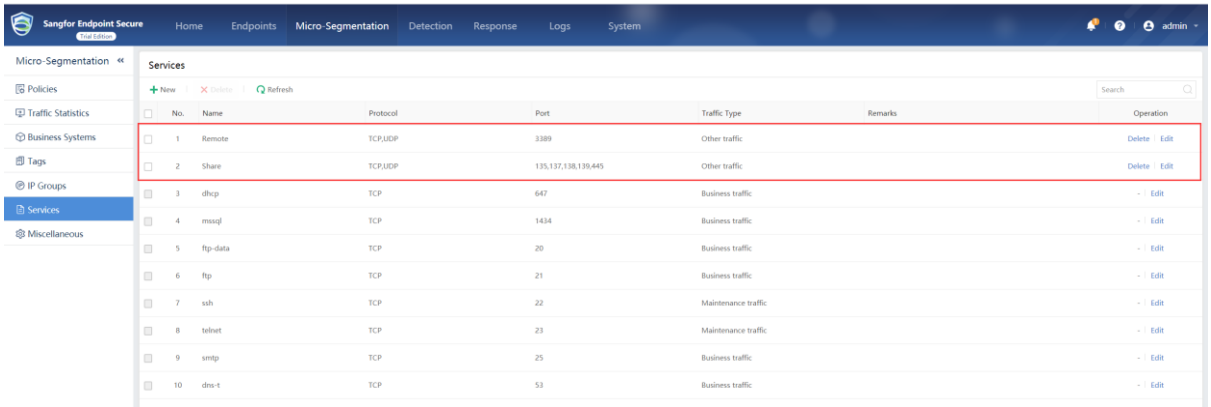


3.Gunakan metode yang sama untuk menambahkan Business System Windows2 lainnya dan pilih spesifik endpoint.



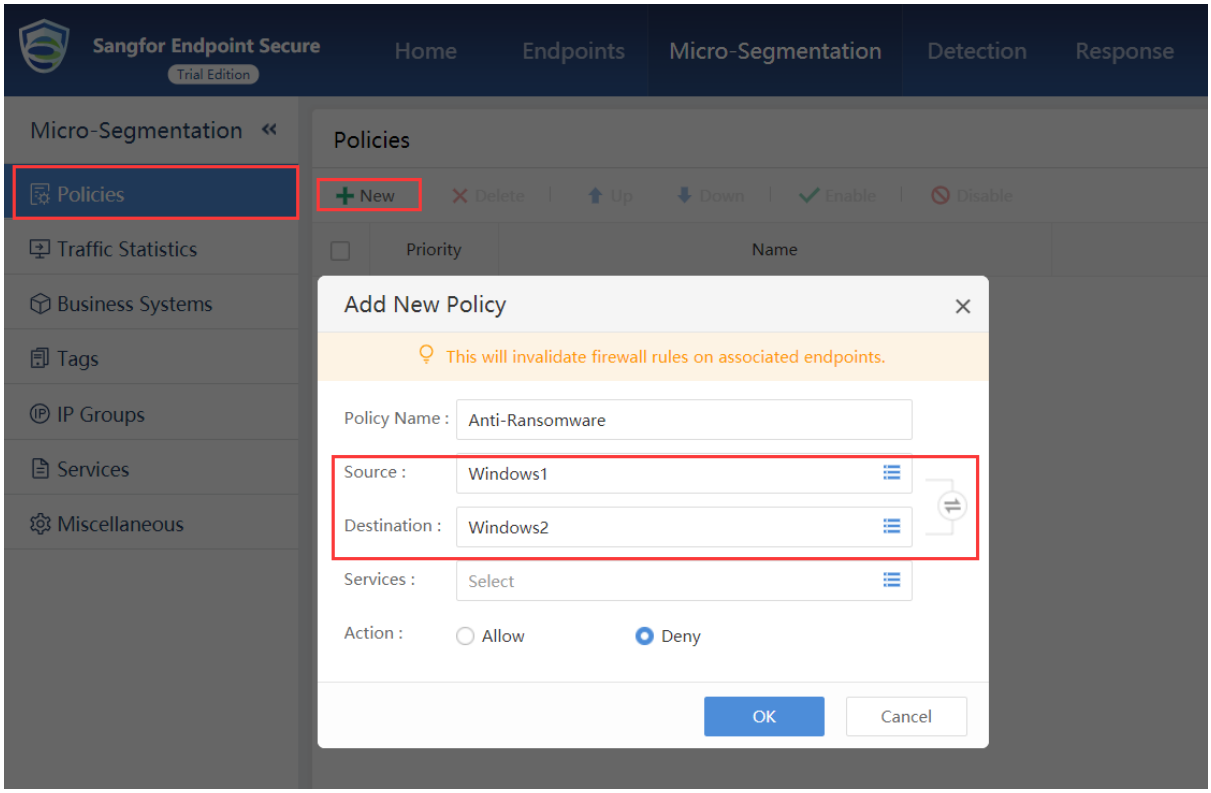
3.2 Tentukan Services

1.Micro-Segmentation module mempunyai beberapa built-in services, tapi kalian dapat mengubah service secara manual. Seperti anti ransomware, kalian dapat membuat beberapa service yang mana termasuk port yang mana ransomware gunakan untuk brute force attack.

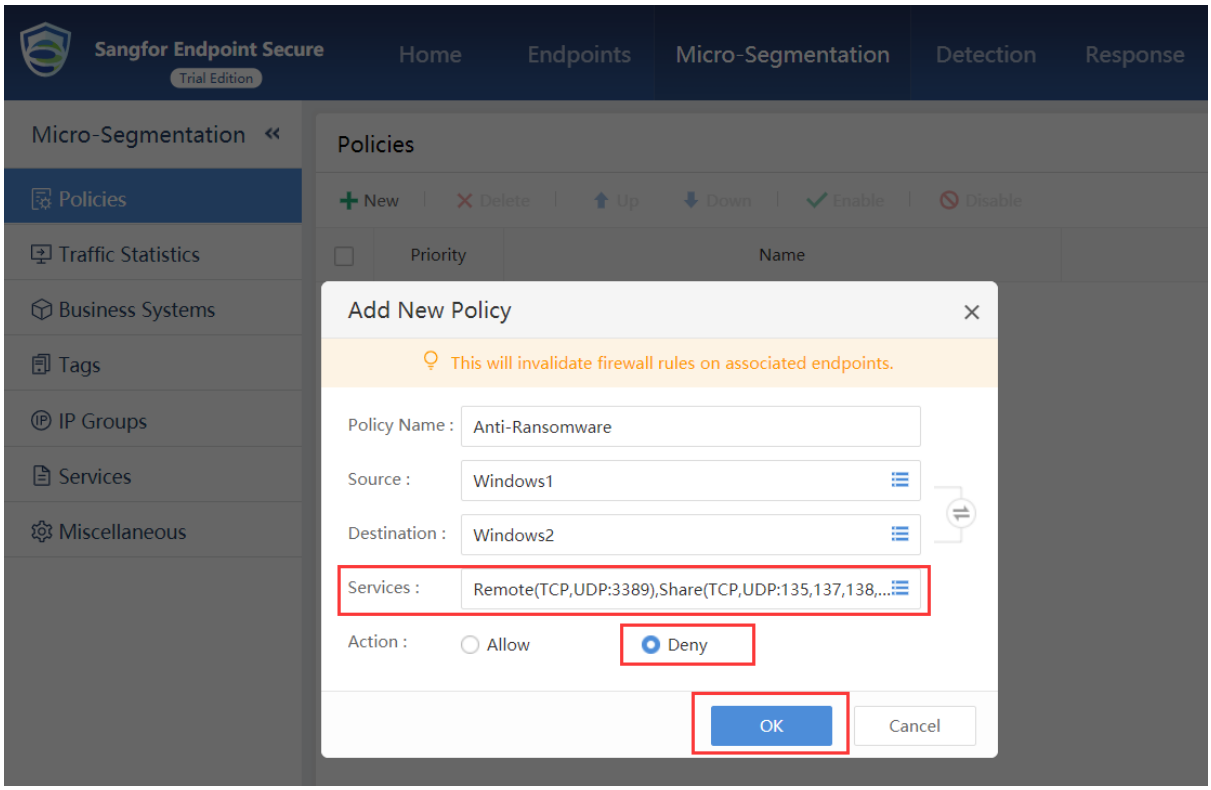


3.3 Buat Micro-Segmentation Policy

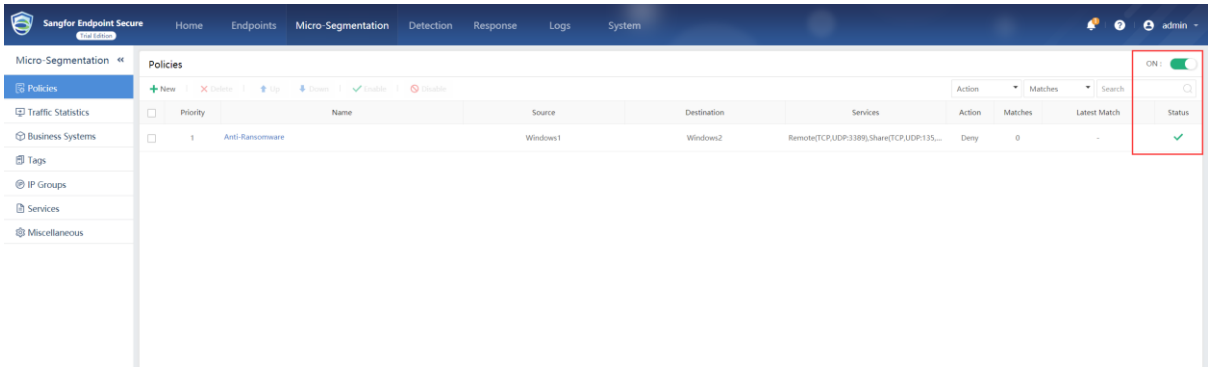
1.Klik Add untuk membuat Micro-segmentation policy, dan pilih Source/Destination Object.



2.Pilih services yang perlu untuk di blok, dan ubah Action as Deny.



3.Pastikan konfigurasi global dan konfigurasi policy enabled.



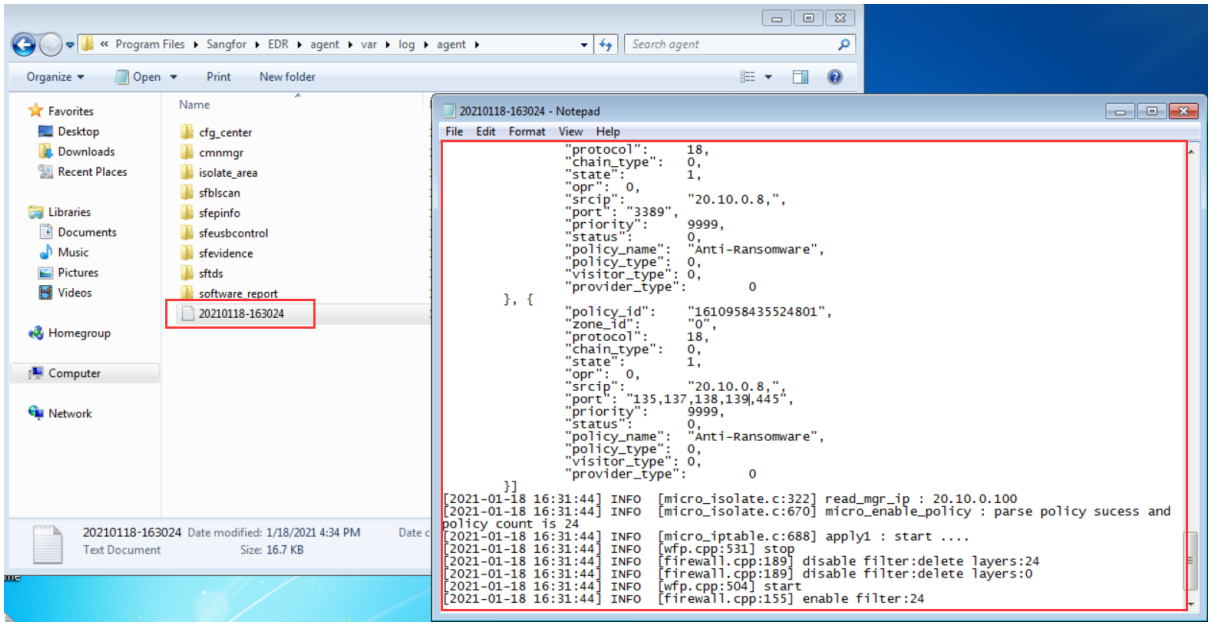
3.4 Periksa Policy Validity

1.Periksa agen log in di endpoint.

Windows Agent log Path：**C:\Program Files\Sangfor\EDR\agent\var\log\agent**

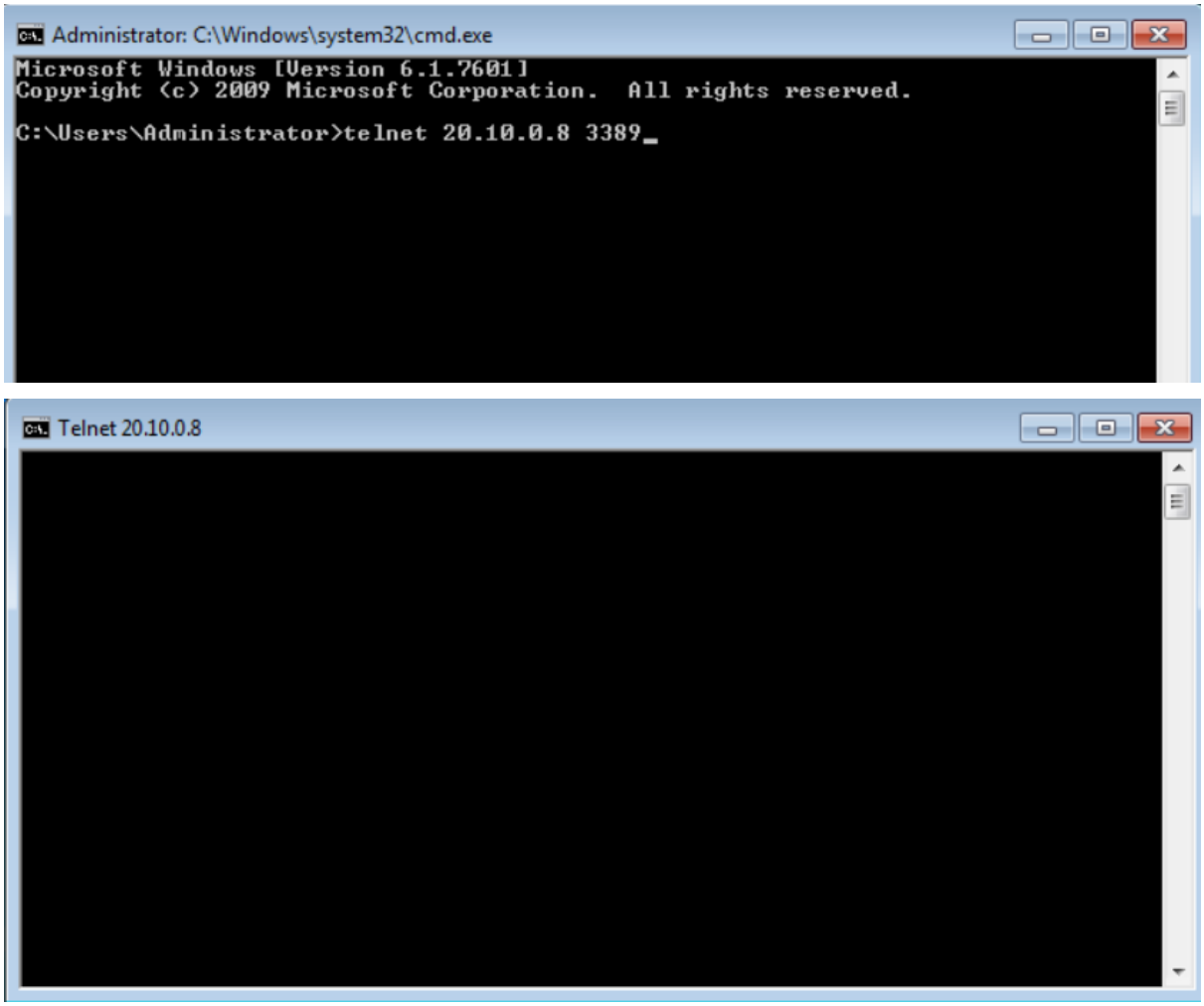
Linux Agent log Path：**/sangfor/edr/agent/var/log/agent**

Jika kalian dapat melihat log sebagai berikut, berarti Micro-Segmentation policy telah berhasil.



2.Gunakan telnet command untuk mengetes konektivitas port.

Sebelum mengaktifkan Micro-segmentation policy.



Setelah mengaktifkan Micro-Segmentation policy.