SANGFOR

Endpoint Secure
Panduan Awal

Perubahan Catatan

Tanggal	Deskripsi Perubahan
4 September, 2019	Panduan awal rilis.

Daftar Isi

Bab 1 Pendahuluan Endpoint Secure

Endpoint Secure adalah sekumpulan solusi keamanan terminal yang disediakan oleh Sangfor, yang terdiri dari perangkat lunak keamanan endpoint ringan dan perangkat lunak platform manajemen.

Platform manajemen Endpoint Secure dapat menampilkan manajemen aset terminal terpadu, mendeteksi dan membunuh virus terminal, pemeriksaan pemenuhan terminal, manajemen terpadu dari kebijakan kontrol akses isolasi mikro, isolasi dan penanganan sekali klik untuk kebijakan keamanan, dan lokasi ancaman di seluruh jaringan berbasis IOC pada serangan yang sedang marak terjadi.

Software keamanan Endpoint mendukung fungsi-fungsi seperti antivirus, pencegahan intrusi, isolasi firewall, pengumpulan dan pelaporan data, dan pemrosesan sekali klik. Sangfor Endpoint Secure juga mendukung kolaborasi dengan NGAF dan IAM, yang merupakan generasi baru dari sistem perlindungan keamanan.

1.1 Fitur dan Nilai Endpoint Secure

Manajemen aset terminal yang komprehensif: memungkinkan inventaris komprehensif aset terminal seluruh jaringan, termasuk terminal server layanan dan terminal PC pengguna. Inventaris menunjukkan nama, alamat IP, alamat MAC, organisasi, pemilik, nomor aset, dan lokasi aset dari setiap perangkat terminal. Informasi aset di setiap terminal harus jelas, dan setiap peristiwa keamanan harus ditangani oleh karyawan tertentu sehingga manajemen keamanan dapat diterapkan.

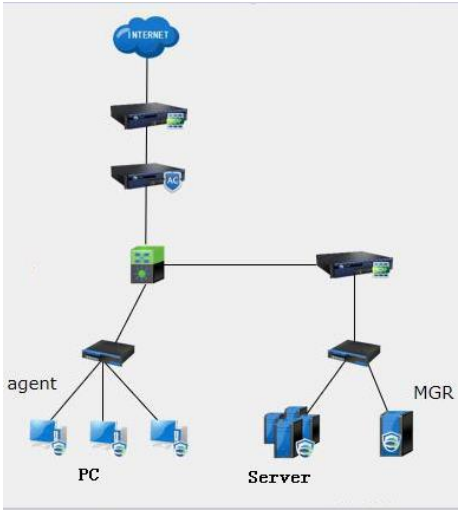
Tinjauan Compliance pada keamanan terminal: Setiap organisasi memiliki persyaratan *compliance* yang unik untuk keamanan terminal, khususnya persyaratan pemenuhan untuk perlindungan kelas dan persyaratan keamanan untuk tuan rumah. Kajian pemenuhan keamanan terminal dirancang sesuai dengan persyaratan keamanan host berdasarkan perlindungan tingkat. Itu melakukan tinjauan pemenuhan pada kebijakan tentang otentikasi identitas, kontrol akses, audit keamanan, pencegahan intrusi dan pencegahan kode berbahaya, yang bertujuan untuk memenuhi persyaratan keamanan host berdasarkan perlindungan kelas untuk perusahaan.

Perlindungan real-time terhadap ransomware: Ransomware adalah jenis malware yang mengenkripsi file korban. Kemudian penyerang meminta tebusan dari korban untuk memulihkan akses ke file setelah pembayaran. Jenis malware ini menjadi semakin populer dan terjadi iocan kecerdasan IOC tentang peristiwa panas berdasarkan analisis keamanan global menggunakan data besar, dan mengirimkan data intelijen ke Endpoint Secure. Endpoint Secure dapat dengan cepat melakukan analisis lokasi pada ancaman di seluruh jaringan berdasarkan data intelijen IOC, dan mendeteksi serta merespons peristiwa panas terbaru tepat waktu. Selain itu, Endpoint Secure melakukan analisis akar penyebab berdasarkan data perilaku historis untuk melindungi organisasi dari peristiwa keamanan.

1.2 Pendahuluan Deployment

The Endpoint Secure digunakan pada pengguna lokal dan Agen diinstal pada setiap server. Endpoint Secure ditautkan dengan Sangfor Security Cloud melalui jaringan publik. Agen di setiap server di LAN dihubungkan dengan Endpoint Secure. Dengan cara ini, pengguna terminal lokal diberikan kecerdasan dan solusi keamanan yang akurat. Semua data dienkripsi dalam proses komunikasi. Server tidak memerlukan izin untuk mengakses jaringan publik, dengan demikian isolasi keamanan tercapai.

Skenario yang berlaku: server diisolasi dari Internet. Diagram jaringan adalah sebagai berikut:



- Instal platform manajemen Endpoint Secure (MGR) di server Linux.
- Instal program Agen di terminal (Windows dan Linux) untuk deteksi keamanan terminal.
- MGR memberikan kebijakan keamanan kepada Agen untuk melakukan deteksi ancaman dan perlindungan keamanan untuk terminal.
- MGR dihubungkan dengan Sangfor Security Cloud melalui jaringan publik. Agen di setiap terminal di LAN terhubung dengan MGR. Dengan cara ini, pengguna terminal lokal diberikan intelijen dan solusi keamanan yang akurat.

Bab 2 Syarat Instalasi

Bab ini menjelaskan kondisi instalasi untuk manajemen pusat Endpoint Secure (selanjutnya disebut MGR) serta klien (selanjutnya disebut Agen). Endpoint Secure tidak melibatkan produk perangkat keras.

2.1 Central Management End (MGR)

MGR tempat sistem Linux diinstal harus dikonfigurasi sebagai berikut:

CPU: > = 4 cores

Memory: > = 8 GB

Hard drive: > = 500 GB

Persyaratan sistem: 64-bit Ubuntu (rekomendasi Ubuntu16 atau diatasnya) or Centos (Centos7 atau diatasnya). Sistem operasi 32-bit atau sistem Windows tidak mendukung. Kondisi di atas juga harus dipenuhi jika mesin virtual pergunakan (platform mesin virtual Sangfor HCI dan VMware juga didukung).

***Catatan: Ketidakcocokan dapat terjadi jika persyaratan sistem tidak terpenuhi.**

Konetifitas Jaringan:

- Agen berkomunikasi dengan MGR melalui port 443, 8083, dan 54120 (port 443 untuk mengunduh Agen, port 8083 untuk layanan, dan port 54120 untuk manajemen).
- Port 443 digunakan untuk akses platform manajemen. Izinkan kebijakan firewall yang sesuai untuk memastikan konektivitas.
- Platform manajemen perlu berkomunikasi dengan server pemutakhiran (121.46.26.113). Harap pastikan konektivitas. Mesin pencari cloud untuk malware Deteksi file perlu mengakses https://analysis.sangfor.com.cn dan https://auth.sangfor.com.cn/v1/auth.

  Pastikan konektivitas antara platform manajemen dan https://analysis.sangfor.com.cn dan

https://auth.sangfor.com.cn/v1/auth. (Kurangnya konektivitas jaringan tidak berdampak pada penggunaan produk tetapi dapat mempengaruhi keefektifan deteksi virus.)

- Untuk meningkatkan produk Endpoint Secure, pelanggan yang secara sukarela bergabung dengan program keamanan cloud perlu mengizinkan https://cloud.sangfor.com.cn untuk pelaporan data virus.

Catatan: Sistem Centos mengaktifkan firewall yang menolak akses ke semua port dalam pengaturan default. Izinkan port yang sesuai diakses oleh konsol.

Jalankan perintah berikut untuk mengizinkan ports 443, 54120, and 8083:

- firewall-cmd --permanent --zone=public --add-port=8083/tcp
- firewall-cmd --permanent --zone=public --add-port=54120/tcp
- firewall-cmd --permanent --zone=public --add-port=443/tcp firewall-cmd --reload

2.2 Endpoint Secure Software (Agent)

Endpoint secure software (Agent) dapat diinstal di sistem Windows 32-bit / 64-bit dan Linux 32-bit / 64-bit umum. Lihat tabel berikut untuk detailnya. Masalah tak terduga dapat terjadi jika sistem yang tidak terdaftar dalam tabel diinstal.

Windows (64bit & 32 bit)		Linux (64 bit & 32 bit)
Server	Pc	Server
Windows Server 2003 SP2	Windows XP SP3	Centos 5,6,7
Windows Server 2008	Windows Vista	Ubuntu 10,11,12,13,14,16,17,18
Windows Server 2008 R2	Windows 7	Debian 6,7,8,9
Windows Server 2012	Windows 8	RHEL 5,6,7
Windows Server 2012 R2	Windows 8.1	SUSE 11,12,16
Windows Server 2016	Windows 10	Oracle Linux5,6,7
Windows Server 2019		

2.3 Pencegahan

- Jika sistem Linux diinstal dengan Agent of Endpoint Secure dan mengaktifkan mikro-isolation, itu akan mengambil alih aturan iptables (fungsi mikro-isolation: aturan iptables yang dikonfigurasi pelanggan dicadangkan dan kemudian dihapus). Jika aturan iptables telah dikonfigurasi, harap berkomunikasi dengan pelanggan terlebih dahulu dan kemudian gunakan fungsi micro-isolation. Menghapus atau menonaktifkan Agen akan memulihkan status firewall asli dan mengambil aturan iptables.
- Saat Agen diinstal di Linux, perintah ping akan digunakan untuk mendeteksi konektivitas dengan MGR. Jika perintah ping mengembalikan kegagalan atau perintah ping dilarang, penginstalan Agen akan gagal.
- Jika sistem Windows diinstal dengan Agen Endpoint Secure dan mengaktifkan mikro-isolation, aturan firewall asli akan terus berlaku dan konfigurasi micro-isolation akan ditambahkan ke firewall.

Bab 3 Instalasi dan Deployment Endpoint Secure

3.1 Instalasi Awal Central Management End (MGR)

3.1.1 Instalasi menggunakan pkg Central Management End (MGR)

Platform deteksi keamanan terminal dan manajemen respons menyediakan paket instalasi offline.

Unduh paket instalasi dari: https://community.sangfor.com

Pilih **[Self-service] - [Software Download] - [Endpoint Secure] - [Endpoint Secure Upgrade Package]**. Unduh paket terbaru untuk penginstalan.

Untuk penginstalan paket offline, pelanggan hanya perlu menyediakan server Linux yang memenuhi syarat (lihat Bagian 2.1 Central Management End (MGR)).

Langkah-langkah instalasi:

- Unduh skrip **manager_deploy.sh** untuk instalasi baru, dan unduh paket instalasi terbaru. Pada langkah ini, paket Endpoint Secure3.2.8R1 pada gambar di atas digunakan sebagai contoh.
- Upload **manager_deploy.sh** dan **Endpoint Secure3.2.8_offline_20181019035239_Build379.pkg** pada direktori manapun di MGR background.
- Jalankan perintah **chmod u+x manager_deploy.sh** untuk mengubah izin ke manager_deploy.sh.
- Jalankan perintah untuk menginstal paket offline: Tunggu sekitar 5 menit hingga penginstalan berhasil.

  ./manager_deploy.sh Endpoint

  Secure3.2.8_offline_20181019035239_Build379.pkg 121.46.26.113

3.1.1.1 Modifikasi Pengaturan Platfom Jaringan

Setelah penginstalan selesai, ubah alamat IP MGR, perutean, dan pengaturan DNS di latar belakang sehingga Agen dapat terhubung ke platform dan platform dapat terhubung ke pencarian cloud dan meningkatkan server melalui Internet.

Langkah-langkahnya adalah sebagai berikut dengan CentOS yang digunakan sebagai contoh:

- Jalankan perintah ifconfig untuk melihat port jaringan.
- Jalankan perintah **vi / etc / sysconfig / network-scripts / ifcfg-eth0** untuk mengubah konfigurasi jaringan.
- Jalankan perintah **vi /etc/resolv.conf** untuk mengubah pengaturan DNS.
- Jalankan perintah restart jaringan layanan untuk memulai ulang layanan jaringan.
- Jalankan perintah **cat /sf/edr/manager/config/server** untuk memeriksa apakah alamat cloud adalah 121.46.26.113. Jika tidak, ubah alamat secara manual untuk memastikan konsistensi. Kemudian, jalankan perintah restart **sh / sf / edr / manager / bin / eps_services** untuk memulai ulang layanan Endpoint Secure.
- Jalankan perintah iptables **–nv -L** untuk memeriksa apakah konfigurasi firewall mengizinkan port 443, 8083, dan 54120. Jika tidak, izinkan port ini.

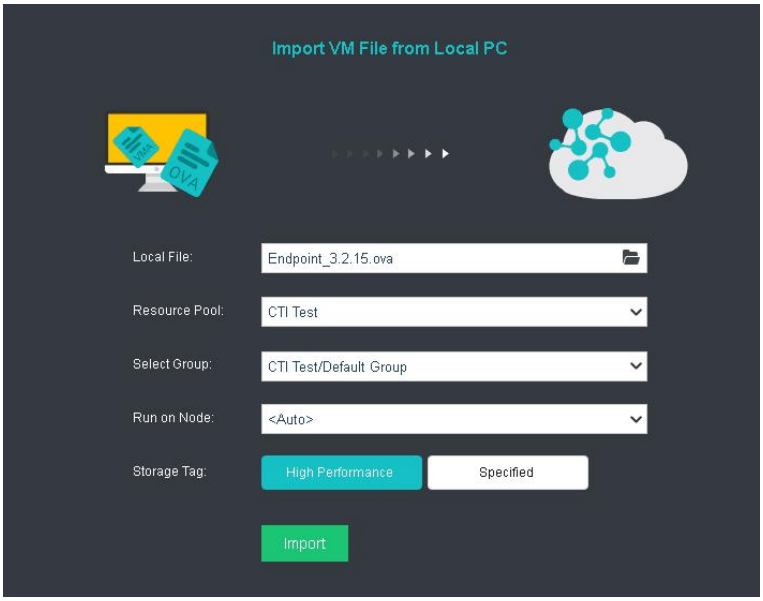
Untuk distribusi Linux lainnya, temukan file yang sesuai dan modifikasi.

3.1.2 Instalasi Central Management End (MGR) menggunakan OVA

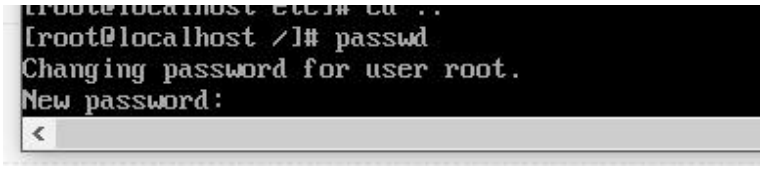
Penerapan template OVA untuk menerapkan MGR di lingkungan virtual VMWARE dan HCI.

Langkah 1: Impor template OVA

Impor template OVA dari lingkungan virtualisasi, seperti yang ditunjukkan pada gambar berikut (menggunakan aCloud sebagai contoh).).



Kata sandi root disarankan untuk diubah (menggunakan perintah passwd) setelah berhasil mengimpor template, seperti yang ditunjukkan pada gambar.



Catatan: Untuk masuk ke backend linux, diperlukan password root.

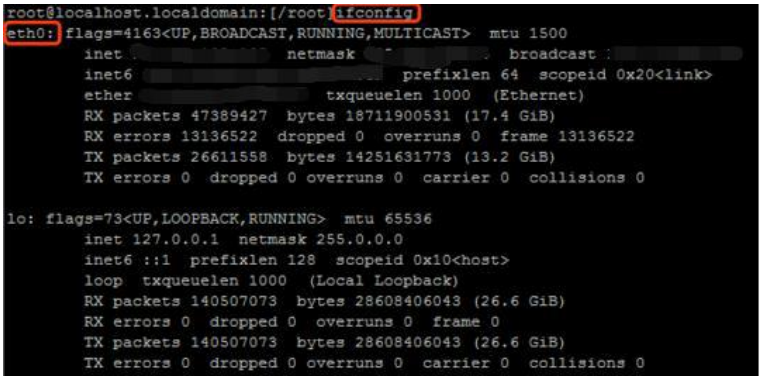
Langkah 2: Kongfigurasi OVA

Ubah alamat IP dan alamat DNS template OVA yang kompatibel dengan jaringan klien.

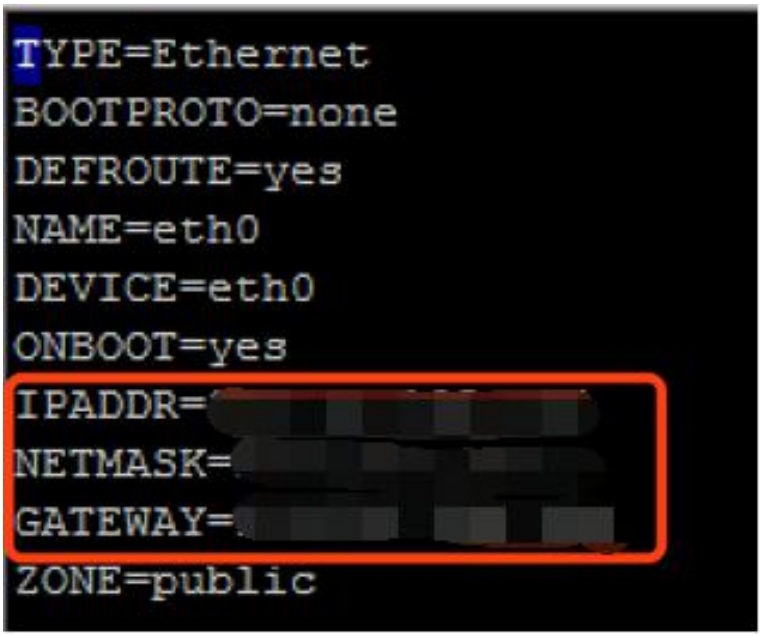
Contoh berikut menggunakan centos, berikut ini hanya bertindak sebagai panduan untuk mengkonfigurasi.

- Ubah alamat IP antarmuka jaringan:

ifconfig atau ip addr untuk memeriksa informasi antarmuka, seperti yang ditunjukkan pada gambar:



Konfigurasikan alamat IP antarmuka, netmask, dan gateway seperti yang ditunjukkan pada gambar:



Ketika konfigurasi selesai, tekan Esc dan jalankan perintah berikut untuk menyimpan dan keluar (: wq!)

- Ubah konfigurasi DNS:

  Ubah konfigurasi DNS untuk memastikan bahwa nama domain berikut dapat diselesaikan dan berfungsi dengan benar.

  (Cloud) Patch terkait kerentanan: https://upd.sangfor.com.cn

  (Cloud) Otorisasi untuk mengakses cloud: https://auth.sangfor.com.cn

  (Cloud) Server analisis cloud: https://analysis.sangfor.com.cn

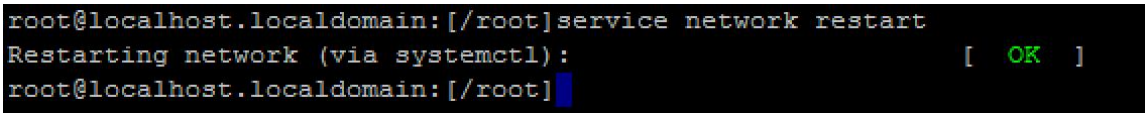
  (Cloud) Paket keamanan cloud: https://clt.sangfor.com.cn

  Jalankan: vi /etc/resolv.conf, konfigurasikan alamat IP DNS di alamat IP server nama, seperti yang ditunjukkan pada gambar:

  Ketika konfigurasi selesai, tekan Esc dan jalankan perintah berikut untuk menyimpan dan keluar (: wq!)

Langkah 3: Mulai ulang layanan agar konfigurasi diterapkan

Jalankan (layanan jaringan restart) untuk memulai ulang jaringan agar konfigurasi dapat diterapkan.



Dari server MGR untuk menguji nama domain yang disebutkan dapat diselesaikan dan konektivitas ke port 443.

3.1.3 Instalasi Central Management End (MGR) menggunakan ISO

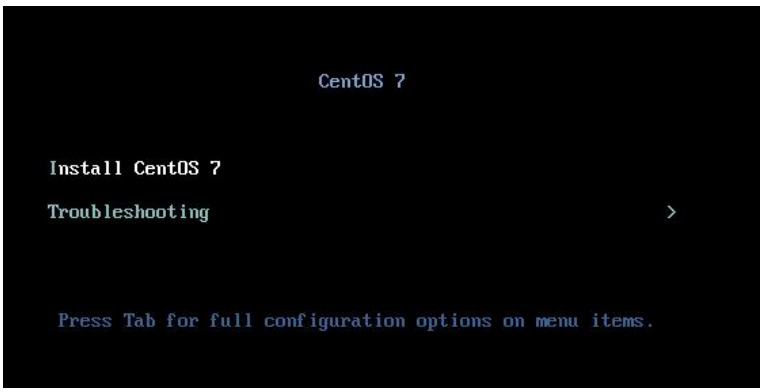
Penyebaran template ISO cocok untuk lingkungan virtual dan server fisik saat menginstal MGR.

Langkah 1: Persiapan untuk pemasangan

File ISO harus siap sebelumnya, kemudian bakar file image ISO ke DVD atau USB.

Langkah 2: Proses instalasi

CD-ROM dan USB harus disetel sebagai urutan boot pertama server. Berikut ini adalah contoh halaman awal.



Pilih “Install CentOS 7”, klik Enter untuk menginstall (proses instalasi akan otomatis), tunggu hingga proses instalasi selesai.

Gambar di atas menunjukkan bahwa instalasi telah selesai, klik "reboot" untuk memulai kembali ke server.

Catatan: Untuk masuk ke backend linux, diperlukan password root.

Langkah 3: Konfigurasi jaringan

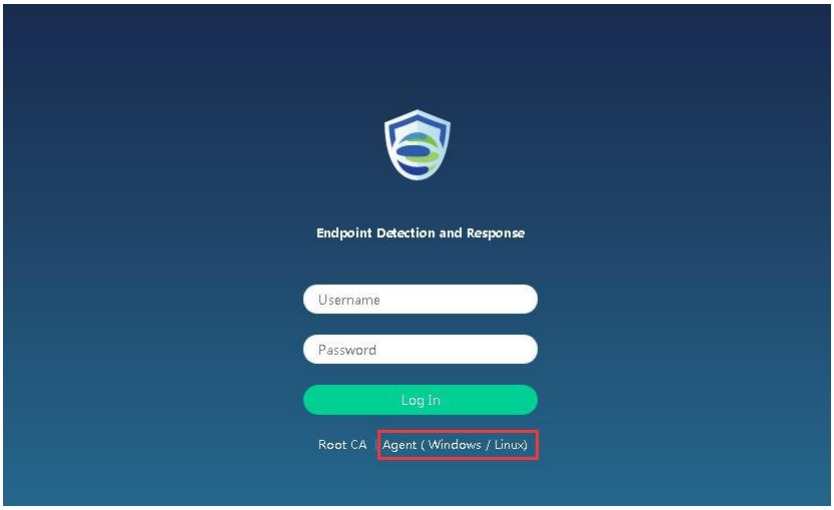
Konfigurasi jaringan termasuk konfigurasi IP, konfigurasi DNS, panduan konfigurasi dapat merujuk ke "3.1.2 Instalasi Central Management End (MGR) menggunakan ova"

3.2 Instalasi Software Endpoint Protection (Agent)

3.2.1 Mengunduh dan Menerapkan Paket Instalasi

3.2.1.1 Menginsatal Agen pada Windows

- Unduh skrip instalasi dari laman konsol MGR (https://Manager_IP). Ada dua konsol yang tersedia untuk mengunduh skrip instalasi.
  1) Laman login.



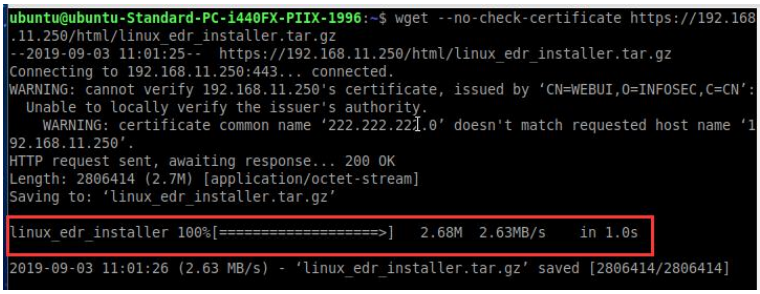
2) Laman sistem menejemen seperti yang terlihat pada gambar.

- Unggah paket instalasi ke perangkat terminal yang akan diinstal, dengan tetap menggunakan nama file. Langsung jalankan file EXE untuk penginstalan. Jalur instalasi perangkat lunak:% ProgramFiles% \ Sangfor \ Endpoint Secure
- Agen akan online di MGR dalam waktu 2 menit setelah penginstalan selesai.

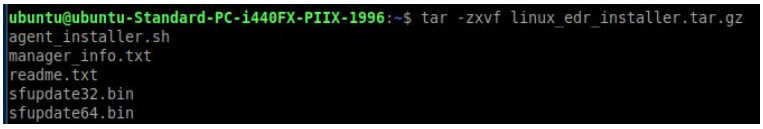
3.2.1.2 Menginstal Agen di Linux

- Unduh skrip instalasi. Ada dua metode pengunduhan, yaitu pengunduhan konsol dan pengunduhan host Linux dengan perintah. Untuk detail tentang pengunduhan konsol, lihat Langkah 1 di Bagian 3.2.1.1 menginstal Agen di Windows.
- Unduh skrip instalasi. Ada dua metode pengunduhan, yaitu pengunduhan konsol dan pengunduhan host Linux dengan perintah. Untuk detail tentang download konsol, lihat Langkah 1 di Bagian 3.2.1.1 menginstal Agent di Windows.
- Unduh skrip instalasi langsung di host Linux dengan menjalankan perintah berikut:

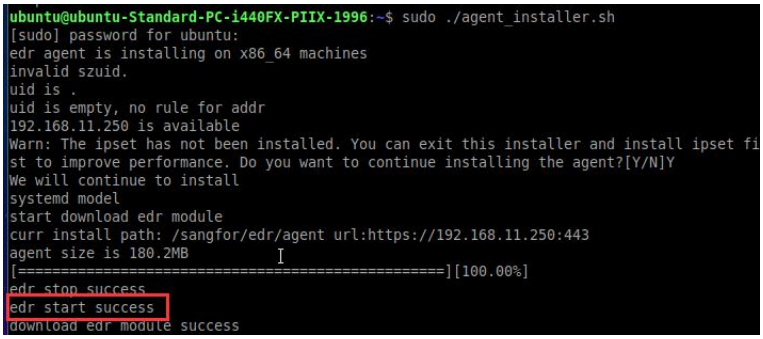
  wget --no-check-certificate https://Manager_IP/html/linux_Endpoint Secure_installer.tar.gz. Berikut perintahnya, Manager_IP mengidentifikasikan alamat IP sebenarnya dari platfom menejemen.



- Unggah skrip instalasi ke perangkat terminal tempat Agen akan diinstal (Lewati langkah ini jika Anda menjalankan perintah untuk mengunduh skrip instalasi). Lalu, jalankan perintahnya **tar -xzvf linux_Endpoint Secure_installer.tar.gz** untuk mendekompresi file.



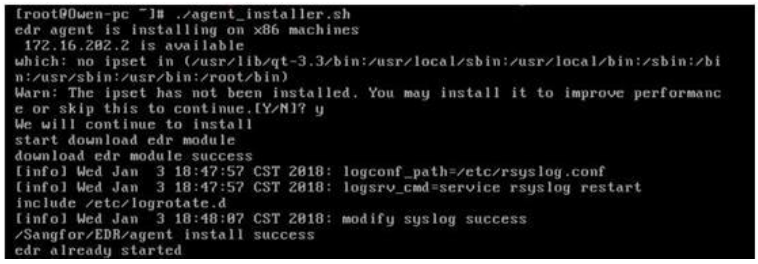
- Jalankan perintah install. Yaitu, jalankan perintah ./agent_installer.sh di direktori terdekompresi untuk menginstal Agen. Secara default, jalur penginstalan adalah /Sangfor/EndpointSecure/agent.



Pelanggan juga dapat menentukan jalur pemasangan. Misalnya, jalankan

./agent_installer.sh 10.251.251.251 /home/Endpoint Secure/ perintah untuk menginstal Agen di / home / Endpoint Secure /. Dalam perintah ini, **10.251.251.251 menunjukkan alamat IP platform manajemen, yang perlu dimodifikasi berdasarkan situasi aktual.**

Proses instalasi akan merekomendasikan instalasi ipset. Anda dapat memilih untuk mengabaikan ipset dan terus menginstal Agen. Jika Anda memilih n, Anda akan mulai menginstal ipset secara manual, dan kemudian menginstal ulang Agent setelah ipset diinstal.



1. Jika sistem Linux diinstal dengan Agent of Endpoint Secure dan mengaktifkan mikro-isolation, itu akan mengambil alih aturan iptables Linux (fungsi mikro-isolation: aturan iptables yang dikonfigurasi pelanggan dicadangkan dan kemudian dihapus). Jika aturan iptables telah dikonfigurasi, harap berkomunikasi dengan pelanggan terlebih dahulu dan kemudian gunakan fungsi mikro-isolation. Menghapus atau menonaktifkan Agen akan memulihkan status firewall asli dan mengambil aturan iptables.
2. Agen akan online di daftar terminal online di MGR dalam waktu 2 menit setelah instalasi berhasil.

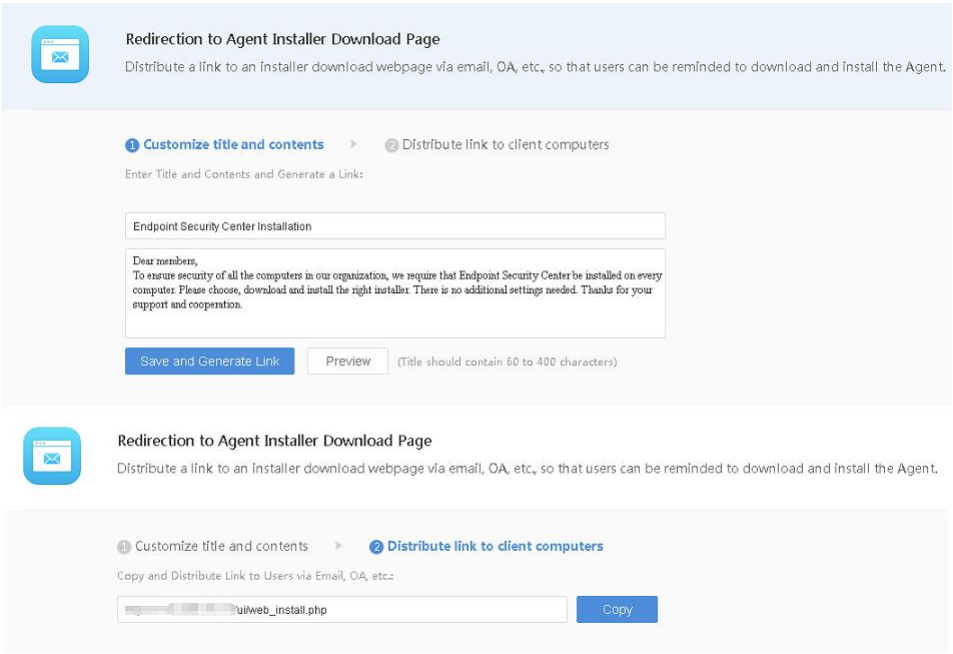
3.2.2 Installing and Deploying the Agent in Batch Mode

3.2.2.1 Webpage Promotion Deployment

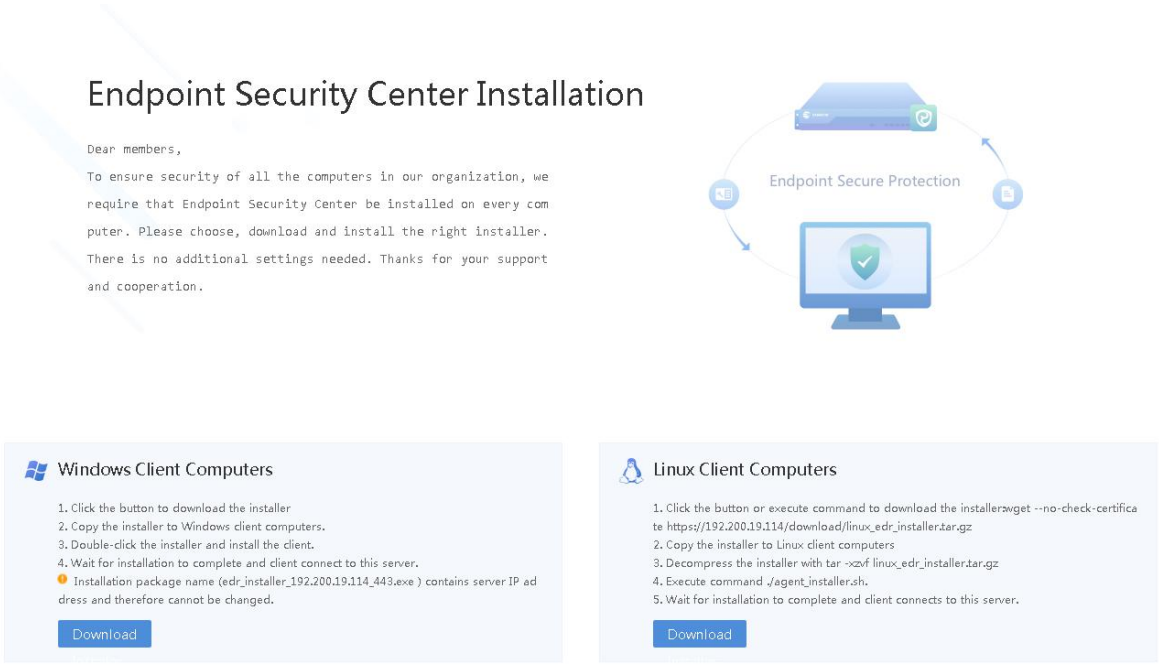
Administrator merilis halaman web pemberitahuan penerapan dan mengirimkan tautan halaman web ke terminal menggunakan email, OA, dll.

Pengguna terminal mengunduh paket penginstalan Agen untuk penginstalan dan penyebaran.

Masuk ke konsol dan pilih [System] - [Clinet Enforcement] - [Redirection to Agent Installer Download Page]. Isi judul dan konten pemberitahuan penerapan. Klik Simpan dan GenerateLink.



Halaman web promosi ditampilkan sebagai berikut:



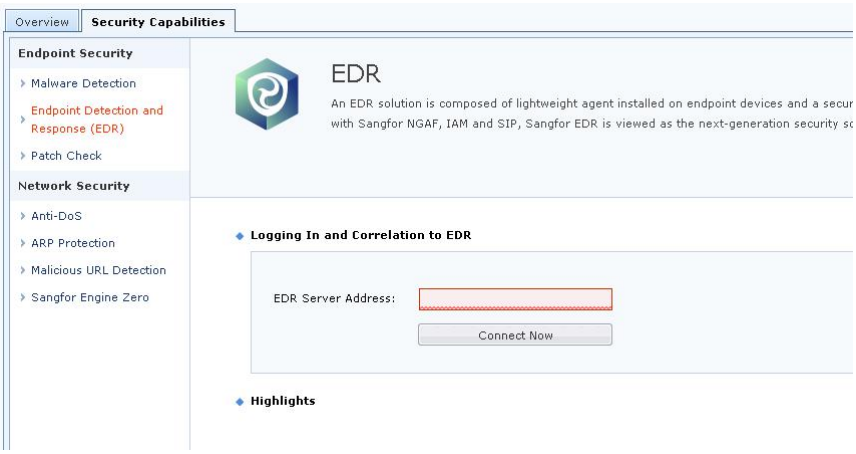
Unduh paket penginstalan Agen. Untuk detailnya, lihat Bagian 3.2.1 Mengunduh dan Menerapkan Paket Instalasi.

Terminal yang akan diinstal dengan Agen memerlukan port 443 untuk mengakses MGR untuk mengunduh program Agen.

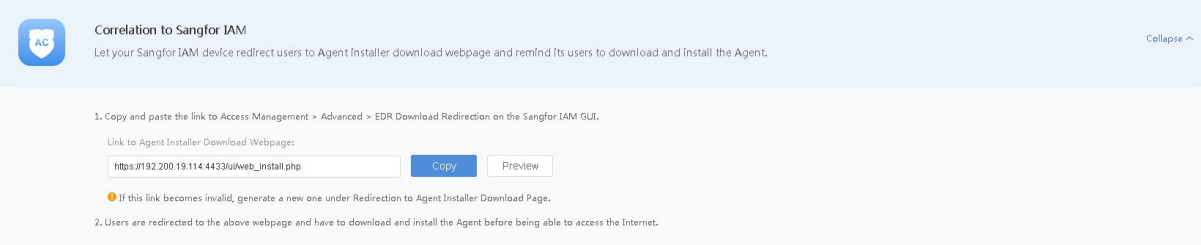
3.2.2.2 Internet Access Management (IAM) Correlation Deployment

Penyebaran agen dapat dikorelasikan dengan sistem Manajemen Akses Internet (IAM) Sangfor. Jika terminal belum diinstal dengan Agent of Endpoint Secure dan memerlukan akses Internet, konfigurasi promosi Endpoint Secure dari sistem IAM akan mengarahkan terminal ke halaman web pemberitahuan penerapan.

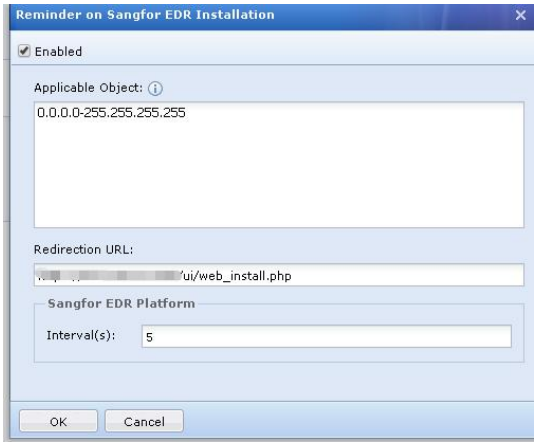
- Masuk ke konsol Endpoint Secure. Pilih [Sistem] - [Correlation], dan lihat perangkat IAM yang terhubung.
- Jika tidak ada perangkat IAM yang terhubung. Masuk ke IAM WebUI lalu [Security] – [Security Cappbilities] – [Security Capabilities] – [Endpoint Detection and Response (EDR)].



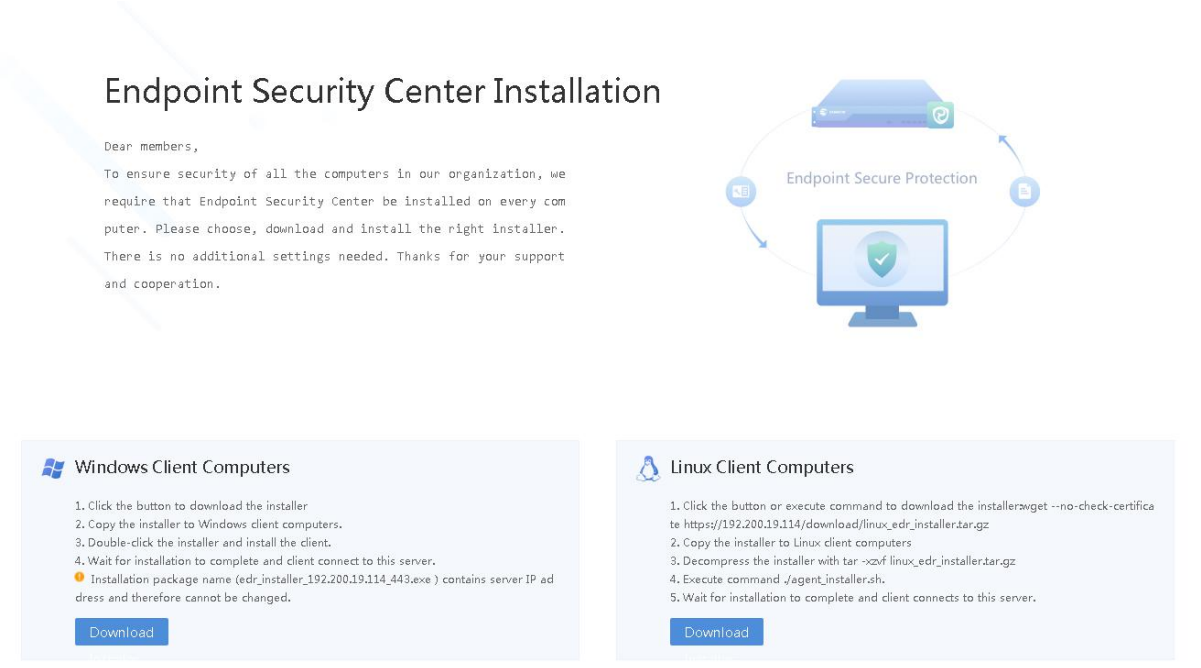
- Pilih **[System] - [Client Enforcement] - [Correlation to Sangfor IAM]**.



- Masuk ke konsol perangkat IAM yang terhubung dengan MGR. **[Security Capabilitiies] - [Security Capabilities] - [Endpoint Detection and Response (EDR)]** untuk pengaturan parameter.
  1) Di kotak teks Cakupan Kebijakan yang Berlaku, isi alamat IP terminal atau segmen alamat IP untuk konfigurasi promosi.
  2) Di kotak teks Redirect Address, isi link yang dibuat pada langkah 3.
  3) Di kotak teks Interval Waktu Dorong, tentukan nilai, yang menunjukkan interval waktu antara dua dorongan berturut-turut dari halaman web unduhan. Selama interval waktu ini, terminal dapat **mengakses Internet secara normal.**



- Di terminal yang akan digunakan, klik browser untuk mengakses Internet.

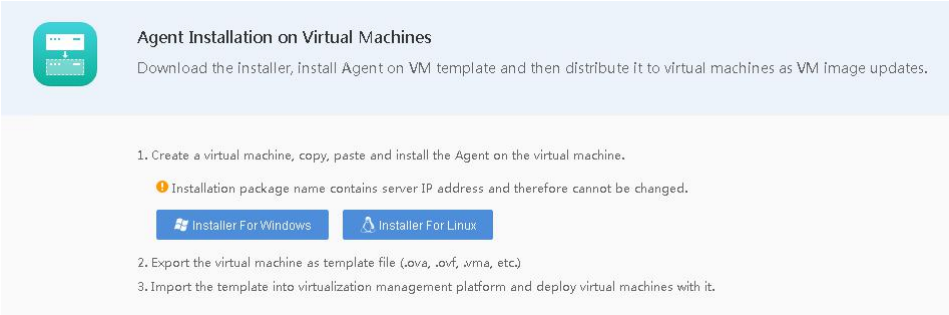


- Unduh paket penginstalan Agen. Untuk detailnya, lihat Bagian 3.2.1 Mengunduh dan Menerapkan Paket Instalasi.

Persyaratan versi IAM minimum: AC12.0.14

3.2.2.3 Virtual Machine Template-based Deployment

Model penyebaran ini berlaku untuk skenario virtualisasi. Administrator melakukan penyebaran cermin dari mesin virtual menggunakan templat mesin virtual pada platform virtualisasi.

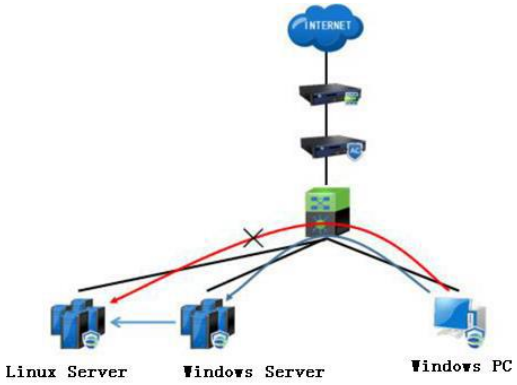


- Buat mesin virtual baru. Instal dan sebarkan Agen di mesin virtual dengan menggunakan paket penginstalan Agen.
- Ekspor mesin virtual sebagai file cermin dalam ova, ovf, vma, atau format lain. Impor file template (file mirror) pada platform virtualisasi, dan terapkan mesin virtual lainnya.
- Alternatifnya, konversikan mesin virtual ke templat yang dapat digunakan untuk mendapatkan mesin virtual dalam batch di platform saat mesin virtual baru diperlukan.

Prosedur untuk mengunduh program Agen di bagian ini sama dengan di Bagian 3.2.1.

Bab 4 Micro-isolation Scenario

Dalam skenario kantor, terminal kantor memiliki izin untuk mengakses server web OA, dan server web memiliki izin untuk mengakses server basis data, sementara terminal kantor tidak memiliki izin untuk mengakses server basis data.



Instruksi:

PC yang berfungsi sebagai Terminal A (diinstal dengan atau tanpa Agen), server Windows yang berfungsi sebagai Terminal B, dan server Linux yang berfungsi sebagai Terminal C (diinstal dengan Agen dan menjaga komunikasi normal dengan MGR)

Interworking jaringan normal antara Terminal A, B, dan C. Anda dapat menjalankan perintah ping untuk memverifikasinya.

Hasil yang diharapkan:

Terminal A (PC) dapat mengakses port 80 Windows Server tetapi tidak dapat mengakses port lain.

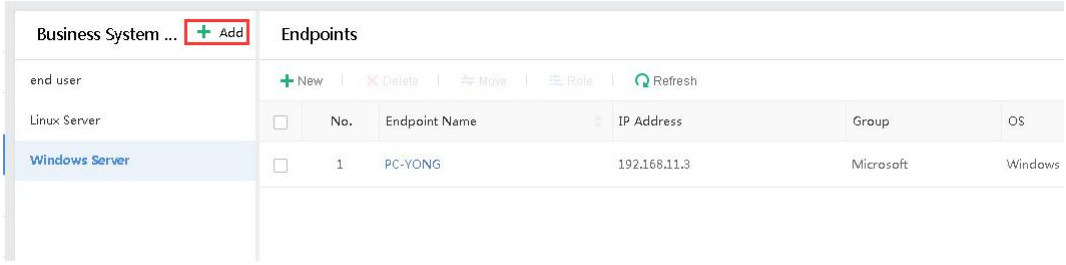
Terminal A (PC) tidak dapat mengakses Server Linux.

Terminal B dapat mengakses port 3306 dari Terminal C tetapi tidak dapat mengakses port lain.Expected Result:

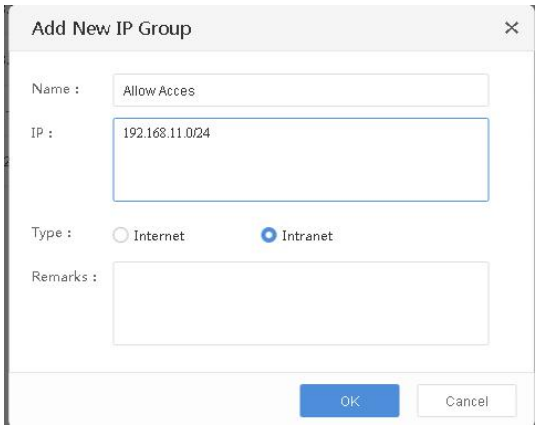
Langkah Konfigurasi:

- Masuk ke MGR. Pilih [Micro-Segmentation] - [Business System] dan klik Tambah untuk membuat

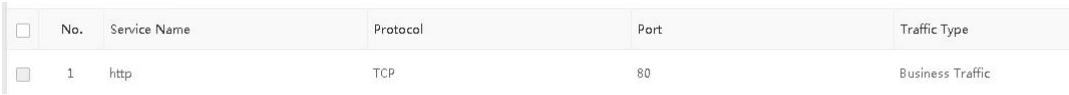
grup sistem bisnis baru. Tambahkan server Terminal B ke OA Windows Server. Tambahkan Terminal C ke sistem server Linux.



- Pilih [Micro-Segmentation] - [IP Group]. Setel kisaran alamat IP untuk terminal kantor yang dapat mengakses web
- Server, dengan nama yang ditetapkan sebagai "Allow Access". Perhatikan bahwa kisaran alamat IP yang ditentukan harus menyertakan alamat IP Terminal A. Pilih Intranet.

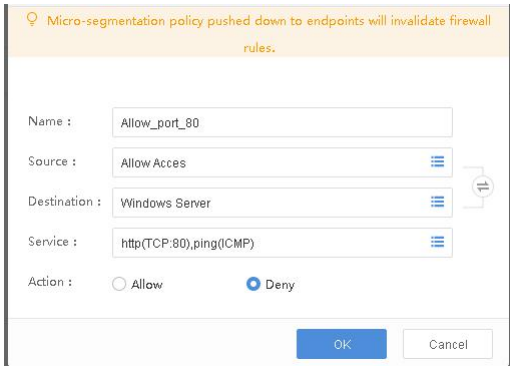


- Pilih [Micro-Segmentation] - [Service]. Anda dapat melihat bahwa port 80 dari server web adalah layanan internal.

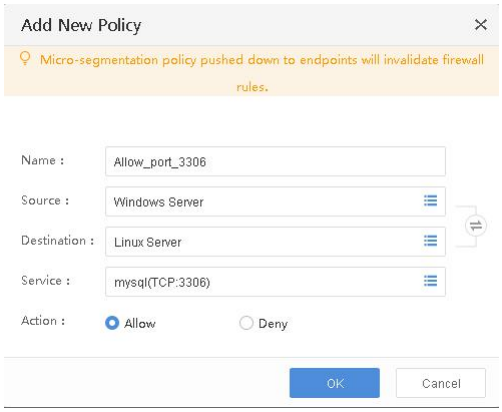


- Database MYSQL menggunakan port 3306 sebagai layanan built-in untuk pengujian.

- Konfigurasikan [Micro-Segmentation Policy] dengan item konfigurasi di atas yang ditentukan. Pilih **Allow** agar Terminal A memiliki izin untuk mengakses Terminal B.



- Pilih **Allow** di kotak dialog berikut sehingga Terminal B memiliki izin untuk mengakses port 3306 dari Terminal C.

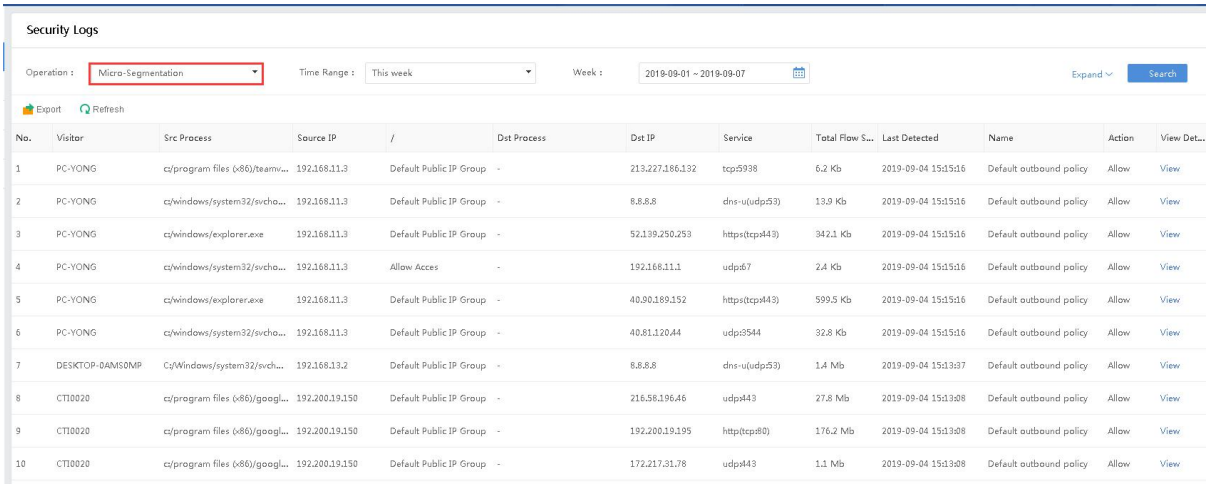


- Lihat status pengiriman kebijakan.

Priority	Name	Source	Destination	Service	Action	Hit Count	Latest Match	Status
1	Allow_port_3306	Windows Server	Linux Server	mysql(TCP:3306)	Allow	0	-	✓
2	Allow_port_80	Allow Acces	Windows Server	http(TCP:80)	Deny	2	2019-09-04 08:45:10	✓

Prioritas pencocokan kebijakan: menambahkan izinkan kebijakan> menambahkan kebijakan penolakan> kebijakan default

- Pilih **[Log] - [Security Log]**. Pilih **Micro-Segmentation** di Jenis Log untuk melihat log Segmentasi Mikro.

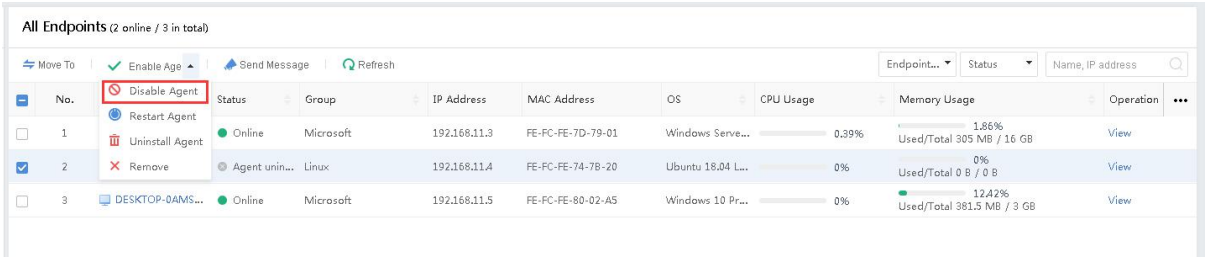


No.	Visitor	Src Process	Source IP	/	Dst Process	Dst IP	Service	Total Flow S...	Last Detected	Name	Action	View Det...
1	PC-YONG	c:/program files (x86)/teamv...	192.168.11.3	Default Public IP Group	-	213.227.186.132	tcp:5938	6.2 Kb	2019-09-04 15:15:16	Default outbound policy	Allow	View
2	PC-YONG	c:/windows/system32/svcho...	192.168.11.3	Default Public IP Group	-	8.8.8.8	dns-u(udp:53)	13.9 Kb	2019-09-04 15:15:16	Default outbound policy	Allow	View
3	PC-YONG	c:/windows/explorer.exe	192.168.11.3	Default Public IP Group	-	52.139.250.253	https(tcp:443)	342.1 Kb	2019-09-04 15:15:16	Default outbound policy	Allow	View
4	PC-YONG	c:/windows/system32/svcho...	192.168.11.3	Allow Acces	-	192.168.11.1	udp:67	2.4 Kb	2019-09-04 15:15:16	Default outbound policy	Allow	View
5	PC-YONG	c:/windows/explorer.exe	192.168.11.3	Default Public IP Group	-	40.90.189.152	https(tcp:443)	599.5 Kb	2019-09-04 15:15:16	Default outbound policy	Allow	View
6	PC-YONG	c:/windows/system32/svcho...	192.168.11.3	Default Public IP Group	-	40.81.120.44	udp:3544	32.8 Kb	2019-09-04 15:15:16	Default outbound policy	Allow	View
7	DESKTOP-0AMS0MP	C:/Windows/system32/svch...	192.168.13.2	Default Public IP Group	-	8.8.8.8	dns-u(udp:53)	1.4 Mb	2019-09-04 15:13:37	Default outbound policy	Allow	View
8	CT10020	c:/program files (x86)/googl...	192.200.19.150	Default Public IP Group	-	216.58.196.46	udp:443	27.8 Mb	2019-09-04 15:13:08	Default outbound policy	Allow	View
9	CT10020	c:/program files (x86)/googl...	192.200.19.150	Default Public IP Group	-	192.200.19.195	http(tcp:80)	176.2 Mb	2019-09-04 15:13:08	Default outbound policy	Allow	View
10	CT10020	c:/program files (x86)/googl...	192.200.19.150	Default Public IP Group	-	172.217.31.78	udp:443	1.1 Mb	2019-09-04 15:13:08	Default outbound policy	Allow	View

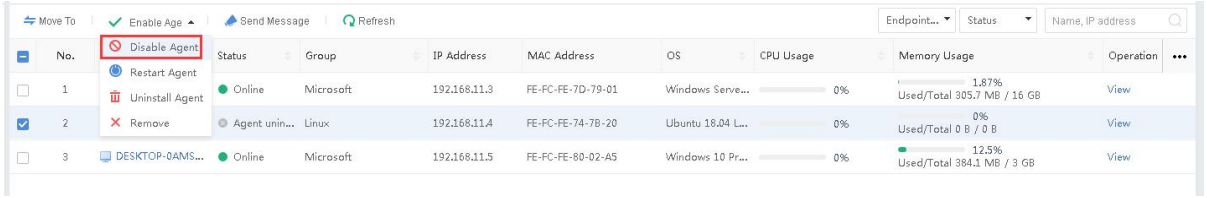
Bab 5 Memastikan apakah Agent memiliki dampak pada System Services

Lakukan langkah-langkah berikut untuk memecahkan masalah terminal jika layanan sistem terminal terkena dampak setelah Agen diinstal:

1. Masuk ke MGR. Tampilkan halaman [Segmentasi Mikro] dan periksa apakah terminal terkait telah mengaktifkan kebijakan segmentasi mikro. Jika demikian, hapus atau nonaktifkan semua kebijakan mikro-segmentasi terminal dari sistem bisnis, dan kemudian periksa apakah layanan sistem terminal kembali normal. Jika layanan masih tidak normal, lanjutkan ke Langkah 2. Jika layanan kembali normal, periksa apakah kebijakan segmentasi mikro yang dikirim ke terminal memblokir beberapa port atau aliran yang dapat memengaruhi operasi normal layanan terminal.
2. Masuk ke MGR. Tampilkan halaman [Endpoint], pilih terminal yang sesuai, dan nonaktifkan fungsi Agen untuk terminal yang dipilih. Kemudian periksa layanan sistem terminal. Jika layanan masih tidak normal, lompat ke Langkah 3. Jika layanan kembali normal, lanjutkan ke Langkah 4.



3. Jika layanan sistem terminal masih tidak normal setelah Agen dinonaktifkan, proses Agen bukanlah penyebab kelainan. Anda tidak disarankan terburu-buru untuk menghapus Agen. Anda dapat menghubungi dukungan teknis Endpoint Secure atau menghubungi layanan hotline (+ 6012-7117129) Sangfor untuk pemecahan masalah. Jika sistem terminal gagal bekerja secara normal, Anda disarankan untuk membuat cadangan log di instalasi Agen terlebih dahulu. directory\Program Files\Sangfor\EDR\agent\var\, dan kemudian hapus instalan Agen. Setelah itu, restart komputer Anda. Jika layanan sistem terminal kembali normal setelah komputer Anda dihidupkan ulang, Anda dapat menghubungi dukungan teknis Endpoint Secure atau menghubungi hotline layanan (+ 6012-7117129) Sangfor untuk pemecahan masalah. Jika layanan sistem terminal masih tidak normal setelah Agen dibongkar dan komputer di-restart, ini menunjukkan bahwa Agen bukan penyebab kelainan.



4. Jika layanan sistem terminal kembali normal setelah Agen dinonaktifkan, Anda tidak disarankan untuk buru-buru mencopot Agen. Anda dapat menghubungi dukungan teknis Endpoint Secure atau menghubungi hotline layanan (+ 6012-7117129) Sangfor untuk pemecahan masalah. Jika Agen harus dicopot dari terminal, Anda disarankan untuk mencadangkan log di direktori penginstalan Agen \ Program Files \ sangfor \ EDR \ agent \ var \, dan kemudian hapus instalan Agen. Anda dapat menghubungi dukungan teknis Endpoint Secure atau menghubungi hotline layanan (+ 6012-7117129) Sangfor untuk mengirimkan log ke personel R&D Sangfor untuk analisis dan pemecahan masalah lebih lanjut.