Endpoint Secure

Best Practices for Scenarios_Use Micro Segmentation to Anti Ransomware

Version 3.2.22

Change Log

Date	Change Description
Feb 25, 2021	Document release.
May 17, 2021	Document update.

CONTENT

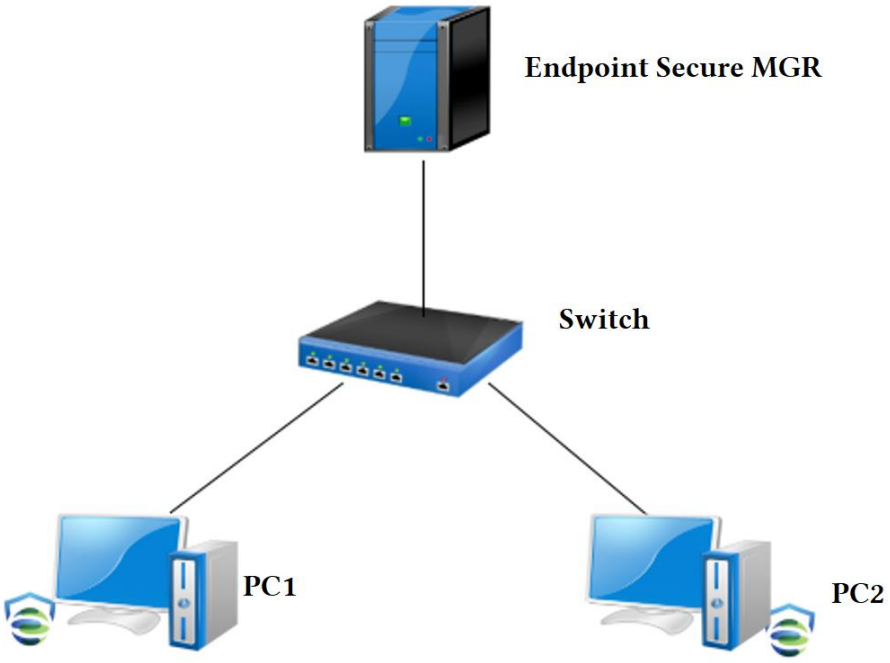
Chapter 1 Overview

This program demonstrates the process and effect of ransomware attacks when the endpoint does not run the Endpoint Secure Agent, as well as the detection and protection effect against ransomware attacks after deploying the Endpoint Secure Agent. It is suitable for showing customers how the Endpoint Secure Agent detects ransomware attacks and provides protection.

Chapter 2 Preparation for Demonstration

2.1 Environment

2.1.1 Network Environment



Device	Account/Password	IP	Description
PC1	administrator/111111	20.10.0.3	PC initiating ransomware attacks
PC2	administrator/111111	20.10.0.8	PC attacked by ransomware with RDP brute-force cracking
MGR	admin/Endpoint Secure@support	20.10.0.100	Endpoint Secure MGR

2.2 Attacking Process

The virus sample is put in C:/windows/evil of PC 1. During the attack, the virus first cracks PC 2 on the same LAN via RDP brute-force attack. After the cracking is completed, computer files on the local PC (PC 1), as well as computer files on PC 2, are encrypted.

2.3 Content

Stage	Content	Expected Result
Round 3	On the Endpoint Secure MGR, enable the protection policy for PC 1 and PC 2 (enabling the micro-segmentation policy to block the sharing ports), and demonstrate the attacking process and effect of ransomware.	1. Files on PC 1 are encrypted by ransomware. 2. PC 2 is protected by the micro-segmentation policy of Endpoint Secure, which blocks virus cracking and spread. As a result, files are not encrypted by ransomware.

2.4 Description

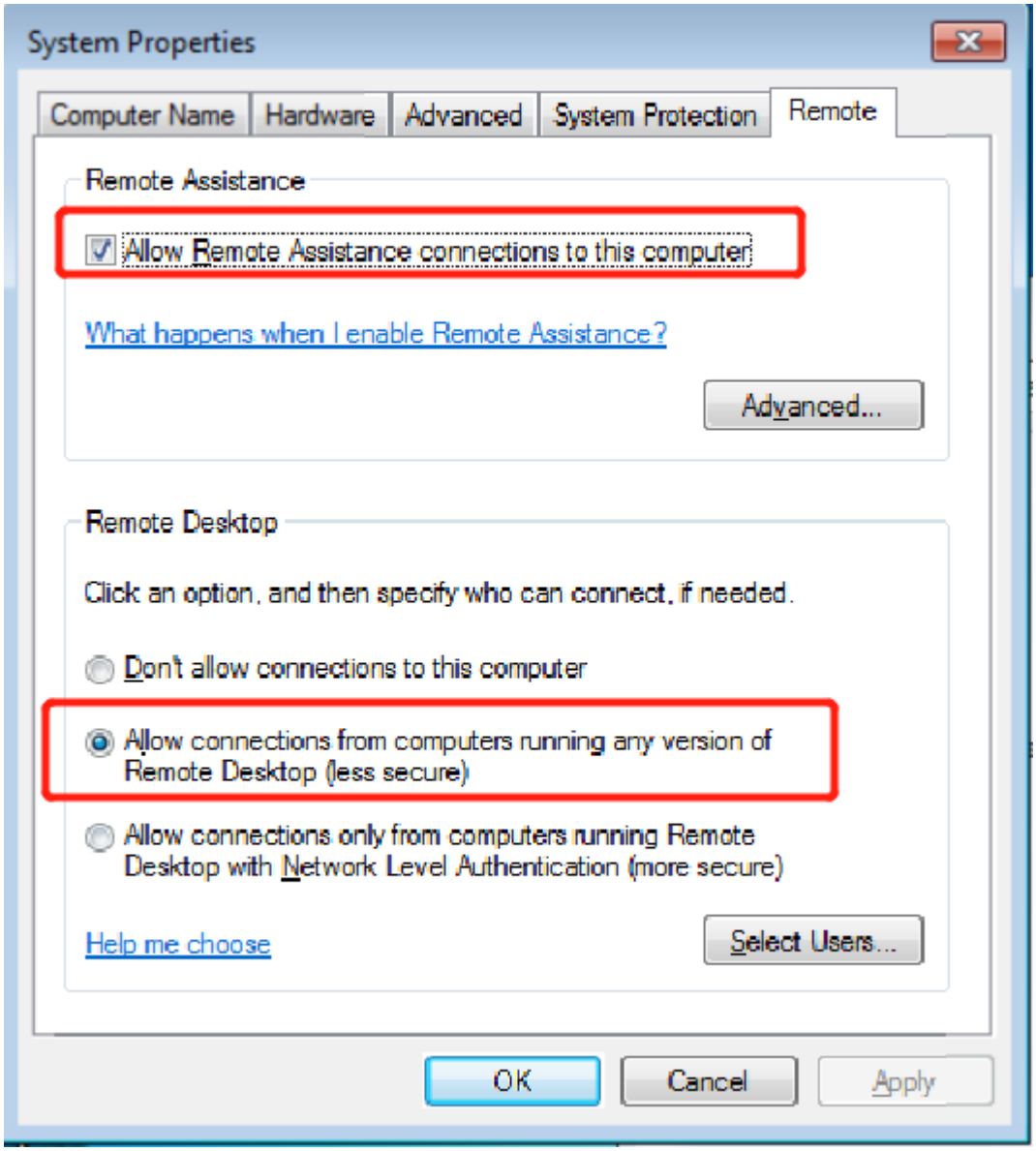
(1) This demonstration is only applicable to the virtualization environment deployed on a client or personal computer, and the demonstration environment needs to be isolated from the customer business network, so as to prevent ransomware from encrypting other computers.

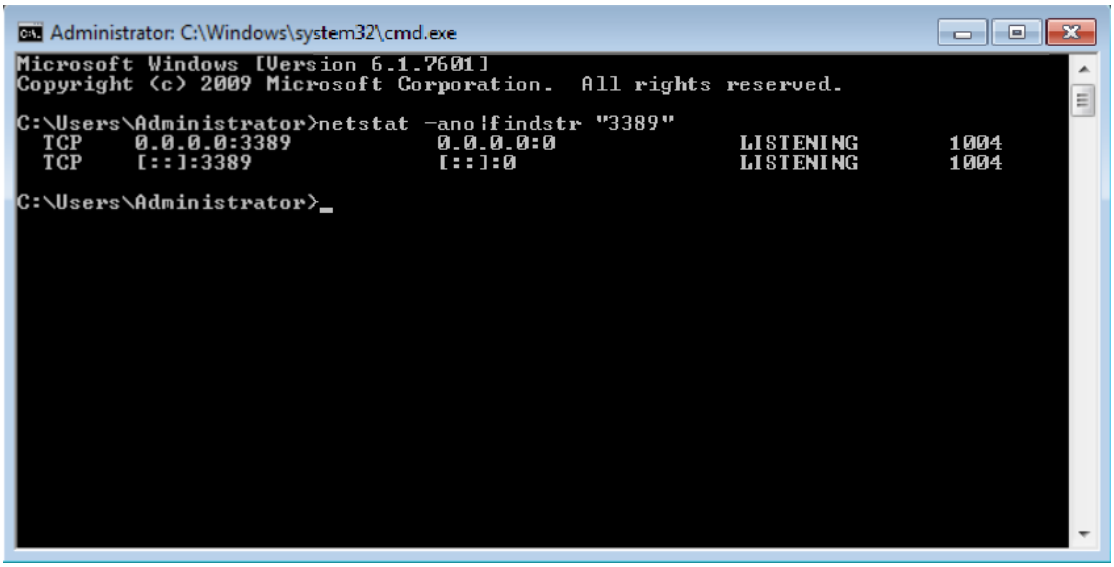
(2) You can set up MGR, PC 1, and PC 2 by yourselves. PC 1 and PC 2 need to install the Endpoint Secure Agent.

(3) Usually, PC 1 and PC 2 run Windows 7 SP1.

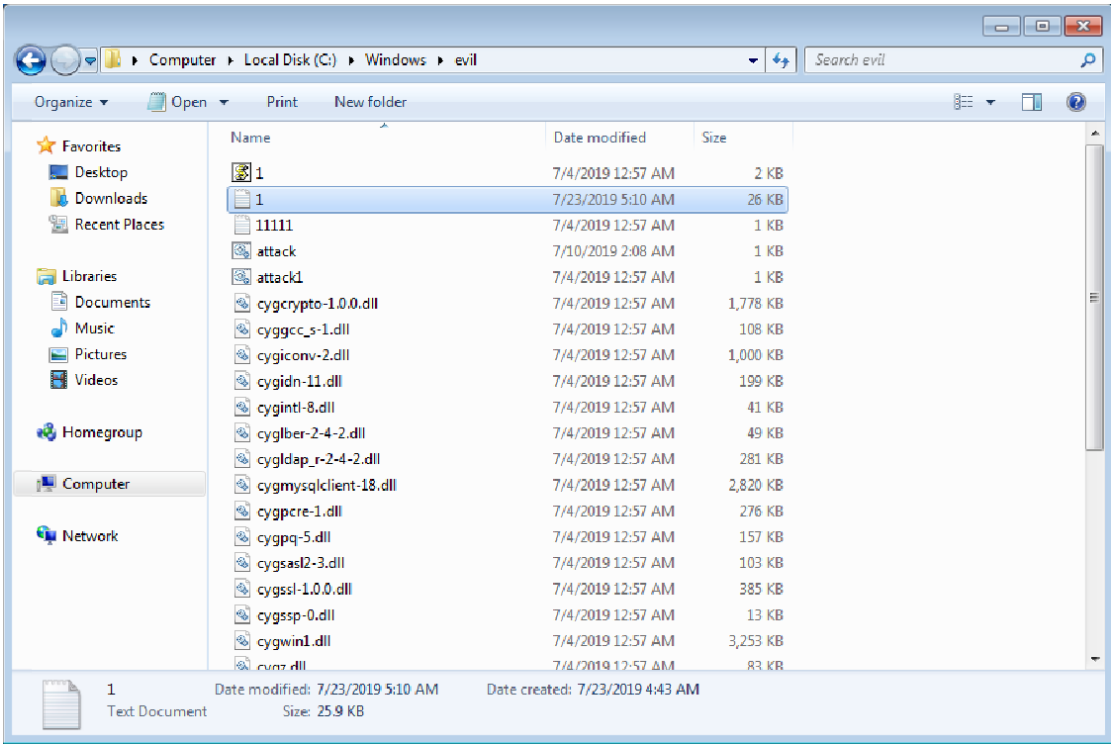
(4) PC 1 and PC 2 can use the addresses of network segment 20.10.0.0/24. The ransomware program will automatically scan other PCs on the same network segment.

(5) You are advised to turn off the system firewall of Windows and enable the RDP service of PC 2 as ransomware will crack through port 3389 of PC 2.

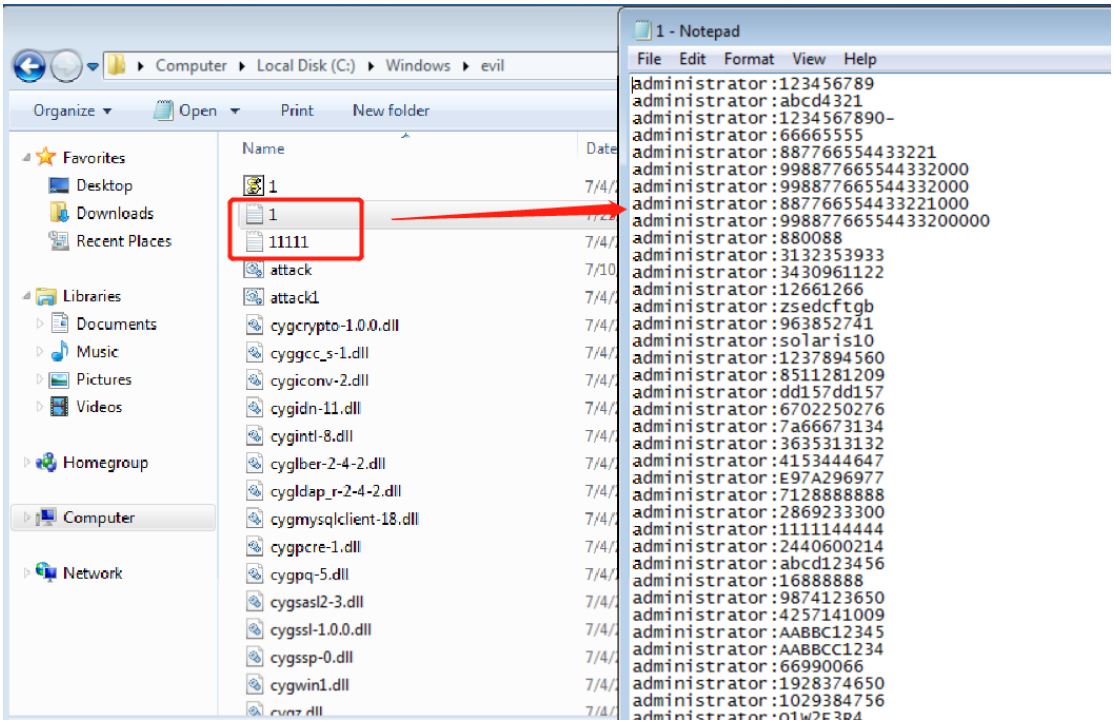




(6) The ransomware sample needs to be put in a specific directory.



(7) Passwords used for virus cracking cover those normally recorded in text files. Therefore, when using your own Windows 7 system, make sure that the passwords used are covered by the text file (containing normal passwords) in the virus toolkit. It is recommended to use administrator/111111 as the username and password.



2.5 Risks

Risk Item	Description
Isolation of demonstration	Since ransomware is run, the demonstration will be

environment	carried out in a virtual environment and needs to be isolated from the real network. If failing to do so, other computer files on the network will be attacked by ransomware.
Snapshot of the PCs used for demonstration	During the demonstration, PC files will be encrypted by ransomware. To quickly restore to the previous status for the next round demonstration, you need to snapshoot the PC in advance.

Chapter 3 Demonstration Process

3.1 Round 3

3.1.1 Content

On the Endpoint Secure MGR, enable the protection policy for PC 1 and PC 2 (enabling the micro-segmentation policy to block the sharing ports), and demonstrate the attacking process and effect of ransomware.

3.1.2 Expected Results

(1) PC 1 files are encrypted by ransomware.

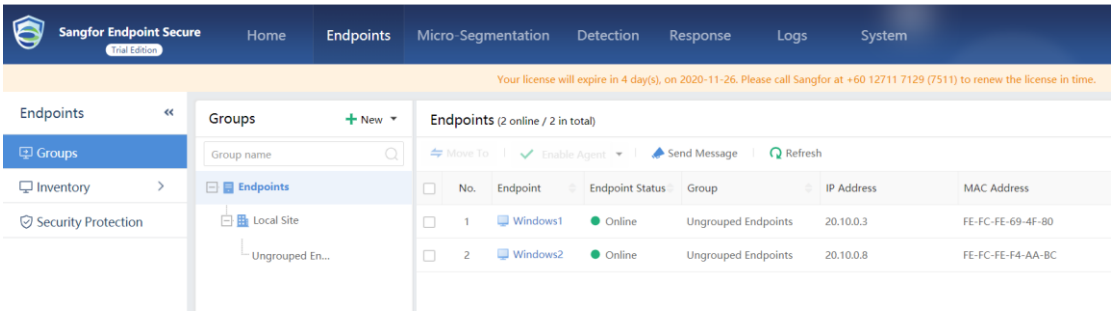
(2) PC 2 is protected by the micro-segmentation policy of Endpoint Secure, which blocks virus cracking and spread. As a result, files are not encrypted by ransomware.

3.1.3 Steps

3.1.3.1 Restoring from Snapshots

(1) Roll back PC 1, PC 2, and Endpoint Secure MGR to the previous status using their snapshots.

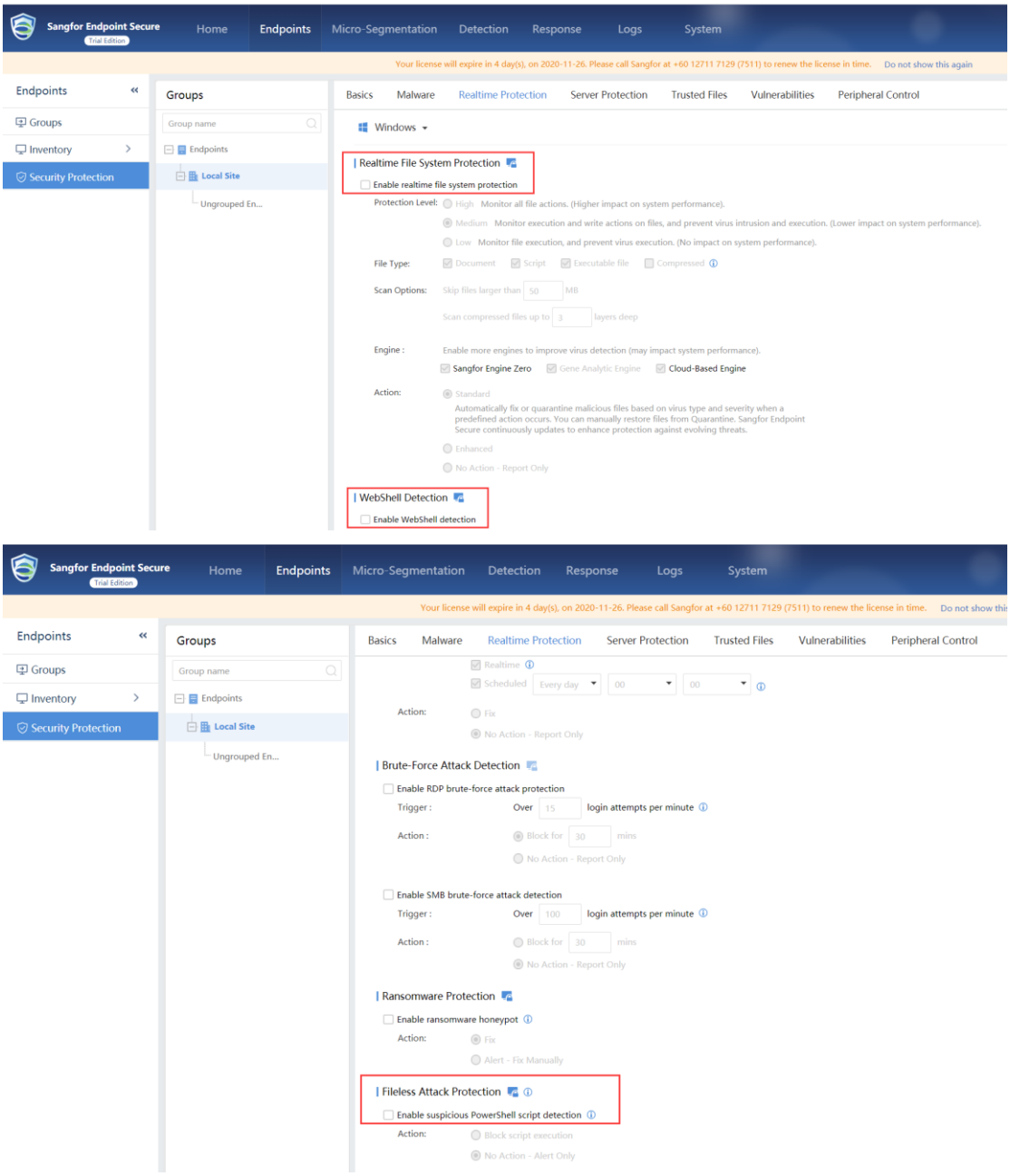
(2) Check Endpoint Secure MGR and find that both PC 1 and PC 2 get online, as shown below:



3.1.3.2 Policy Setting

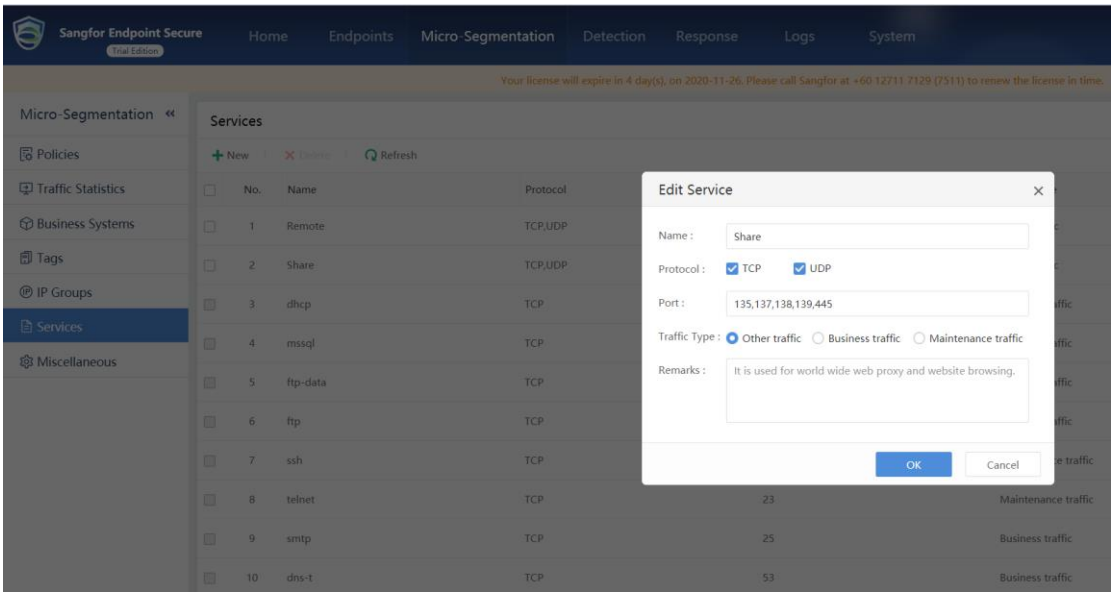
(1) Disable all real-time protection policies.

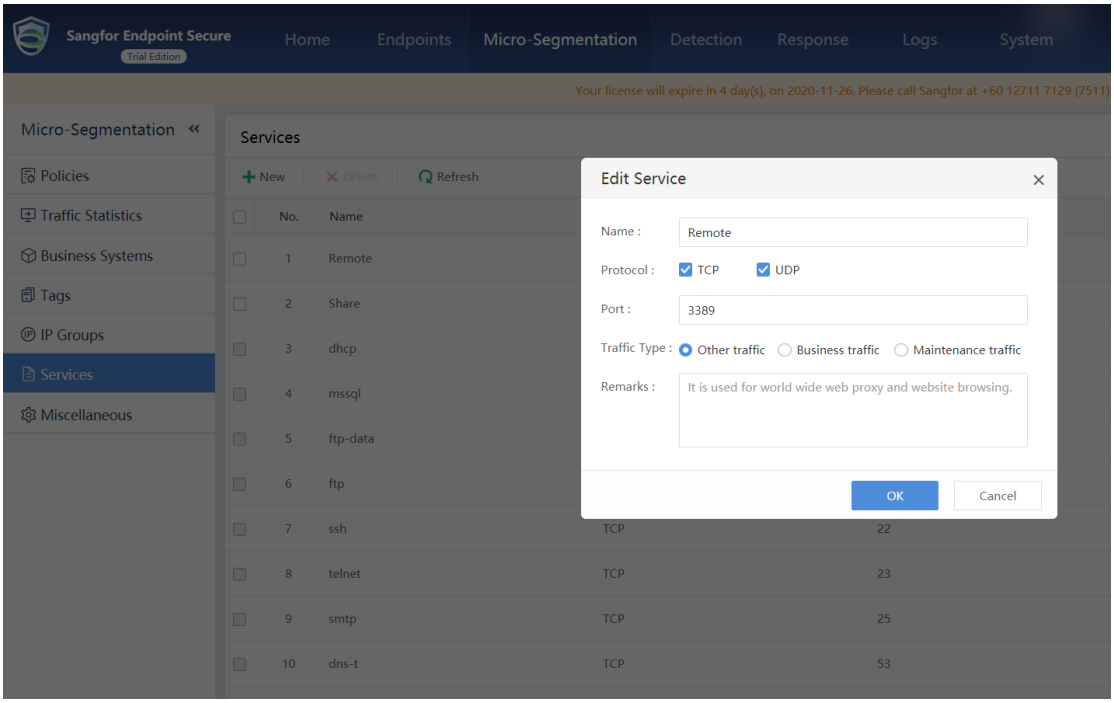
As shown below, choose **Endpoints** > **Security Protection**. Set the **Ungrouped Endpoints** policy and go to the **Realtime Protection** tab. Disable **Realtime File System Protection**, **Ransomware Protection**, **Advanced Threat Protection**, **WebShell Detection**, and **Brute-Force Attack Detection**. Turn on the lock icon.



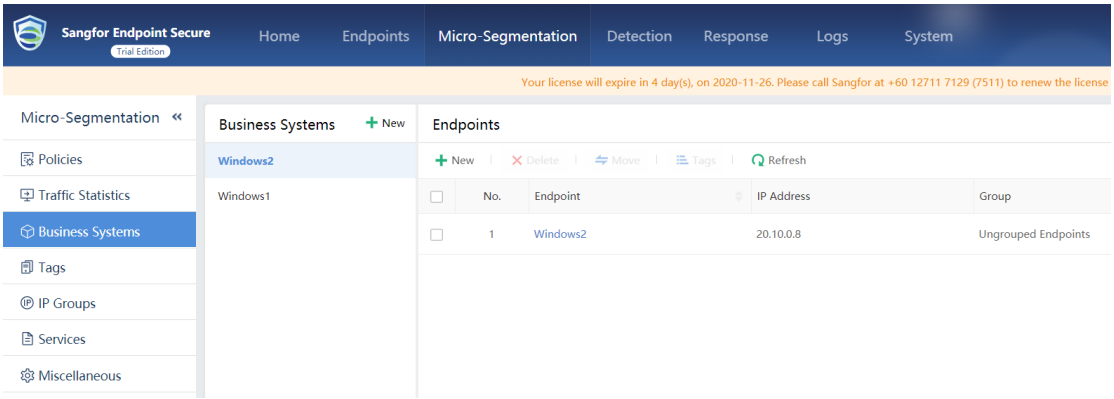
(2) Set the micro-segmentation policy to deny access to the sharing ports and remote desktop of PC 2.

Define the sharing port service. As shown below, choose **Micro-Segmentation** > **Services**. Sharing ports include 135, 137, 138, 139, and 445, and the remote desktop port is 3389.



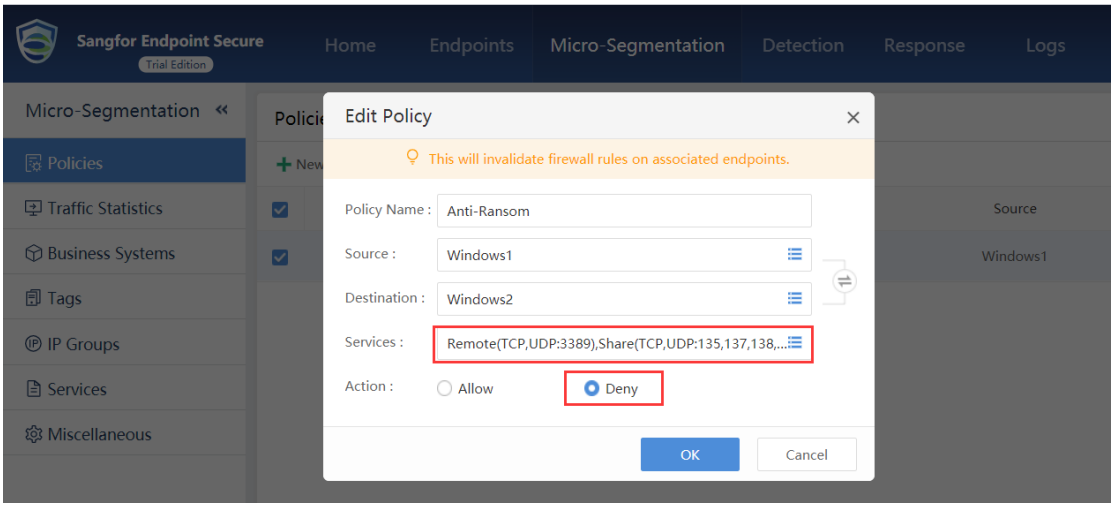


Define the business systems of PC 1 and PC 2. Choose **Micro-Segmentation** > **Business Systems**, as shown below.

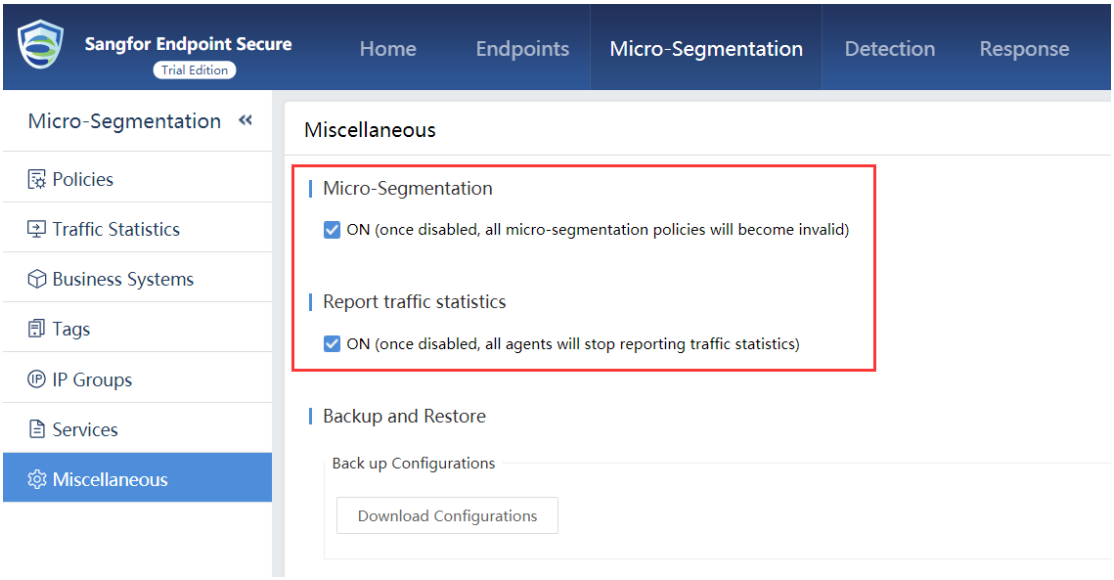


Define the micro-segmentation policy blocking sharing ports, as shown below, to deny PC1's access to

the sharing ports and remote desktop port of PC 2.

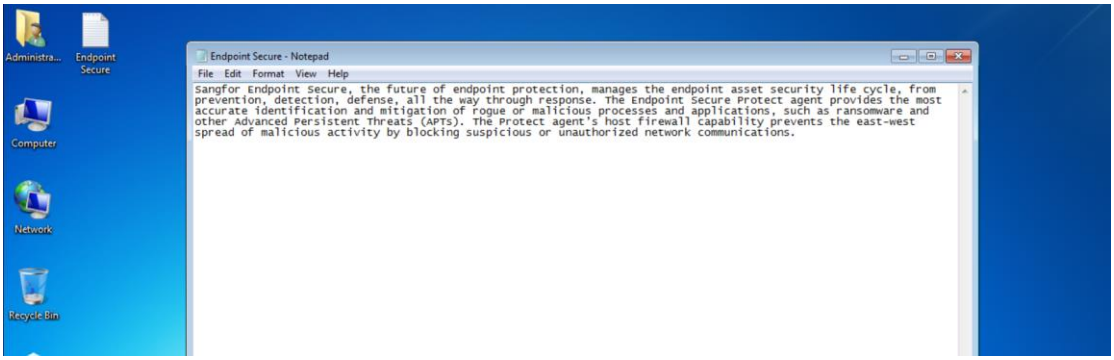


Enable Micro-Segmentation and Report traffic statistics. As shown below, Choose **Micro-Segmentation** > **Miscellaneous**.

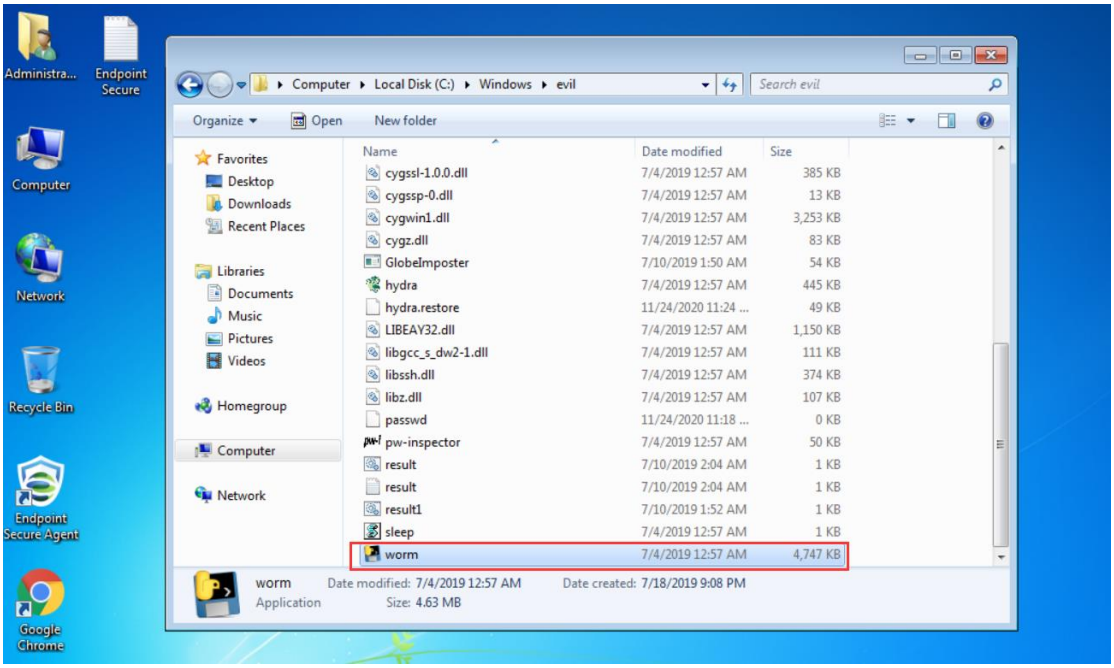


3.1.3.3 Initiating an Attack

(1) Before initiating an attack, check the status of PC 1 and PC 2. Their computer files are not encrypted and can be normally opened, as shown below:



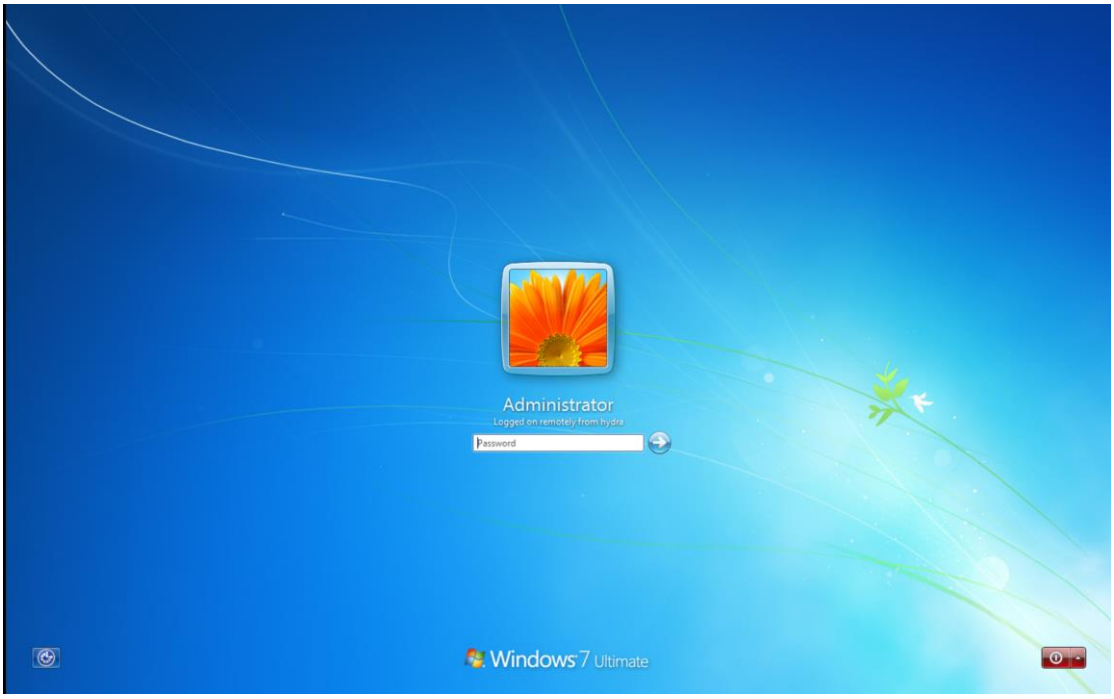
(2) Run ransomware (ready in the OVA environment) on PC 1, as shown below:



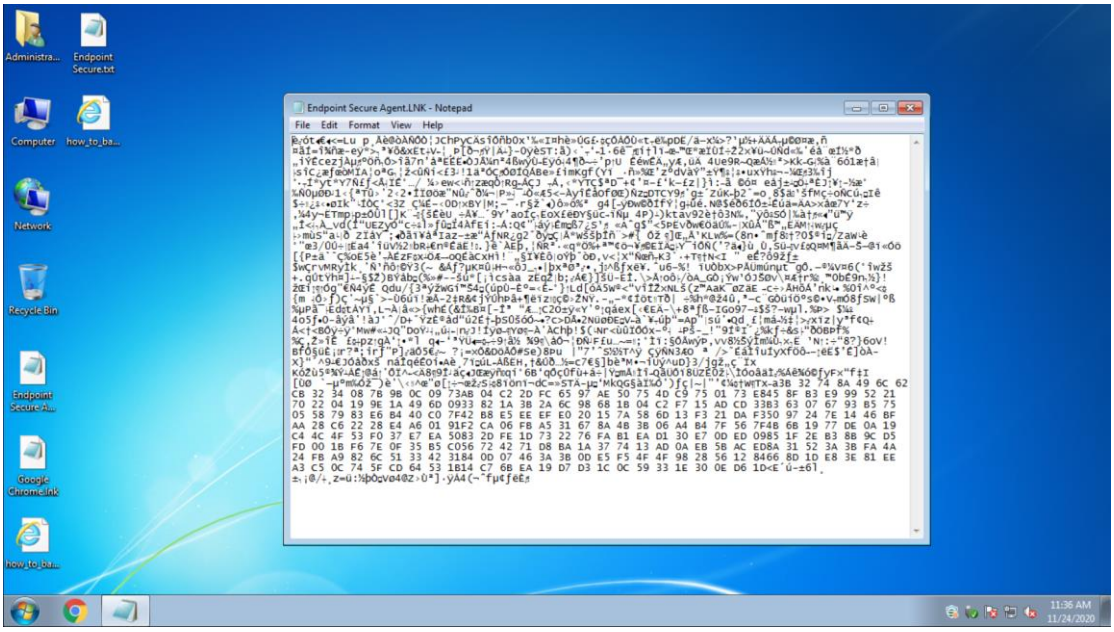
3.1.3.4 Attacking Effect

The attack lasts 2 to 5 minutes. PC 1 is cracked, and computer files on PC 1 are encrypted. For PC 2, the micro-segmentation policy blocks the sharing ports to stop cracking, and computer files on PC 2 are not encrypted by ransomware.

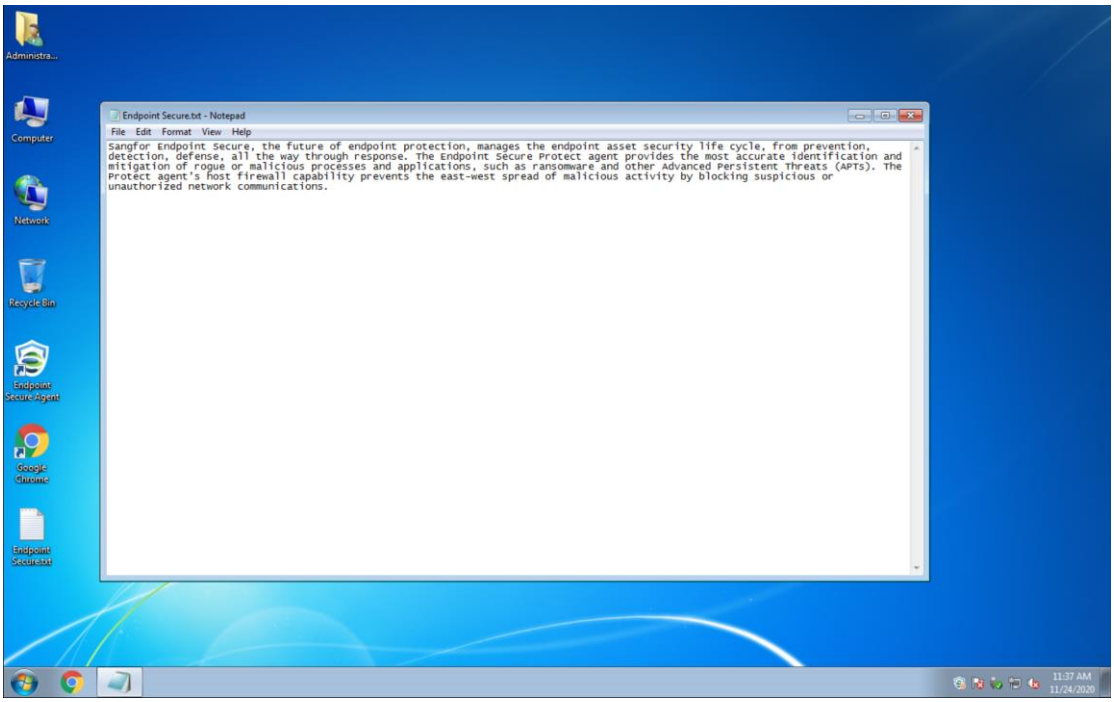
After PC 1 runs ransomware, PC 1 is cracked. Log out and re-log in using administrator/111111, as shown below:



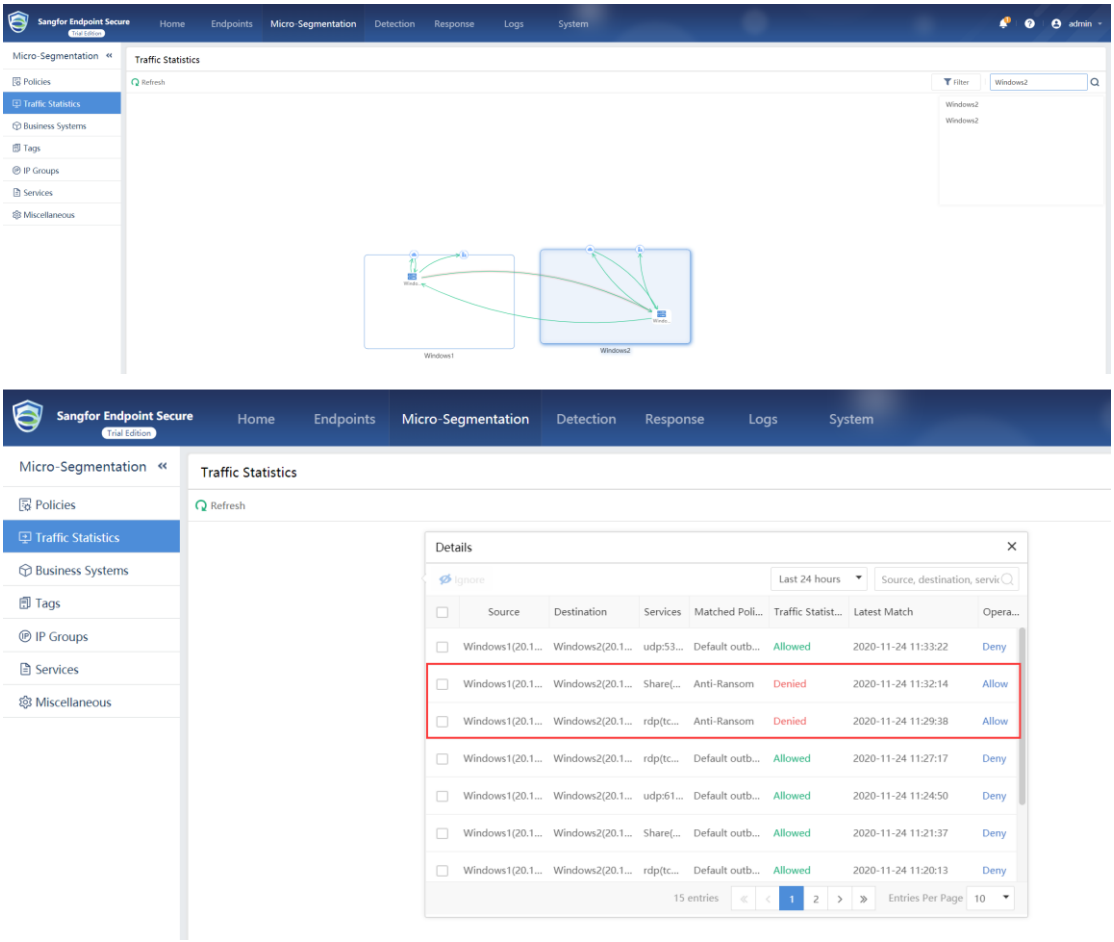
PC 1 runs ransomware, and computer files on PC 1 are encrypted, as shown below:



For PC 2, the micro-segmentation policy blocks the sharing ports to stop cracking, and computer files on PC 2 are not encrypted by ransomware. See the figure below:



View the traffic logs of micro-segmentation. Choose **Micro-Segmentation** > **Traffic Statistics**. Click PC 2 and view its access records. You can find that PC 1's access to sharing ports of PC 2 is denied, as shown below:



Chapter 4 Precautions

1. When the virus program runs, the system may stop responding sometimes and is stuck at the following position for 2 minutes. In this case, you should close and restart the program.