SANGFOR

IAG

Access Check/Control Configuration Guide

Version 13.0.15

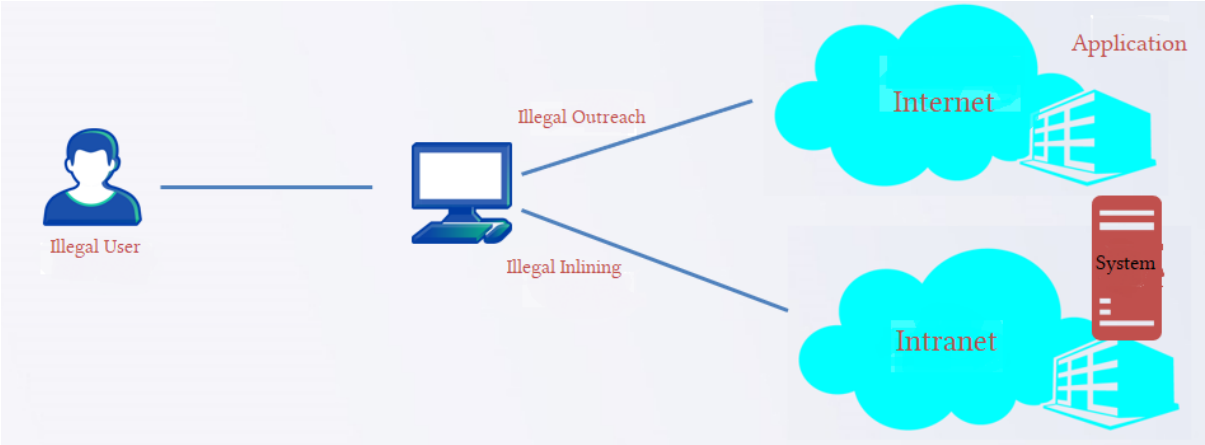
Change Log

Date	Change Description
September 8, 2020	Version 13.0.8 document release.

CONTENT

Chapter 1 Demand Background

- Private network does not allow terminals to connect to other networks to prevent data leakage.
- The terminal has outreach and inline actions, and illegal access cannot be controlled.



Chapter 2 Features Explanation

2.1 Access Check

- Dialup: Determine the dialup behavior by checking the system API interface or function, if exist dialup behavior, it is considered as a violation.

- Network adapter related: By detecting related API interface or function and registry related information to detect whether there is wireless network card, 4G network card and dual network card behavior, if any, consider it as a violation.

- External network: Check whether the following websites can be pinged, if it can be pinged, consider it as able to connect to external networks (www.taobao.com, www.jd.com, www.baidu.com, www.sangfor.com, www.ifeng.com, 5 websites are controlled by the system backend configuration file, which can be modified through the backend).

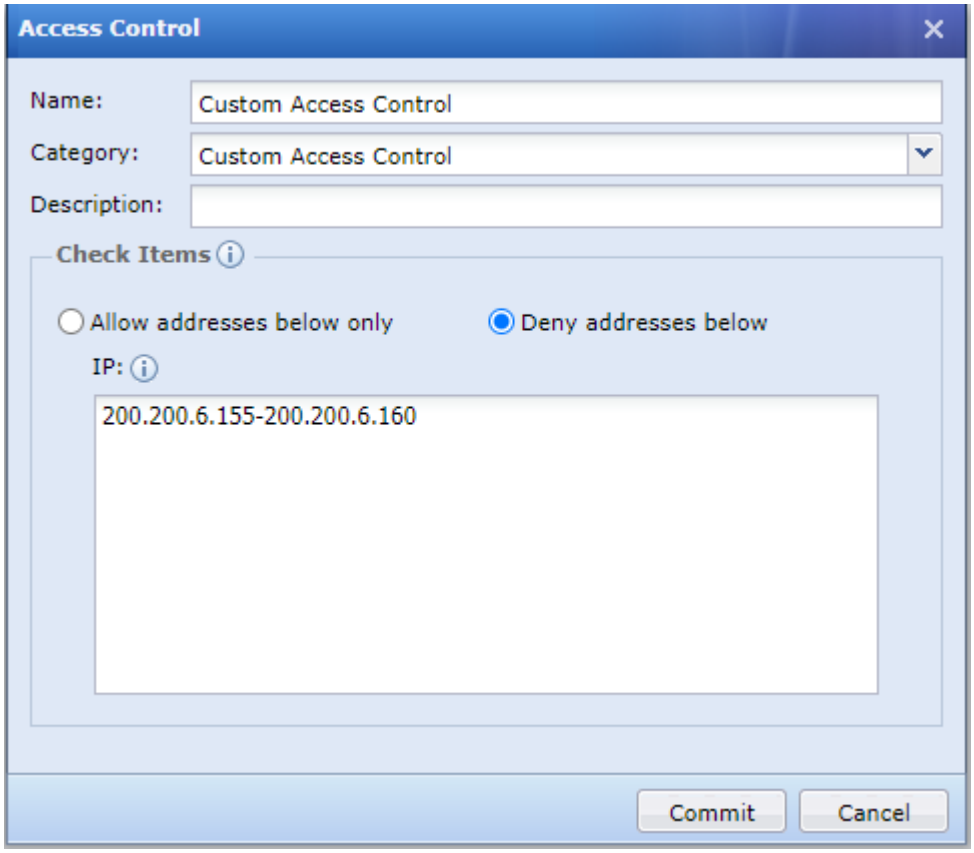
- Unsecured WiFi: Obtain SSID information by checking the API interface or function of the system, then compare with the SSID set in the whitelist, if the connected SSID is not in the whitelist, consider it as a violation.

- Invalid gateway: Obtain all physical network cards by checking the system's API interface or function. The gateway of the network card is compared with the address set in the whitelist. If the gateway of the network card is not in the whitelist, it is considered as a violation.

- Custom: IP/domain name and port can be set, allowing ingress to detect whether it can be accessed, if it can be accessed it is considered to be a violation. When the port is empty, the default is port 80.

2.2 Access Control

- Invoke the Windows system WFP (Windows Filtering Platform) API interface in the framework to achieve micro-isolation function.
- Windows XP PCs do not support management and control (XP does not have a WFP framework).
- Support black and white list, support IP and port, if port is empty the default ports are 1-65535.



Chapter 3 Application Scenario

- Access check/control function is mainly used in private network scenarios, if found that the terminal has illegal access, such as Internet connection behavior, it is blocked by prohibiting the terminal network card.

- Control terminal access permissions through black and white lists, such as only allowing access to a certain IP or prohibiting access to a certain IP range.

Chapter 4 Configuration

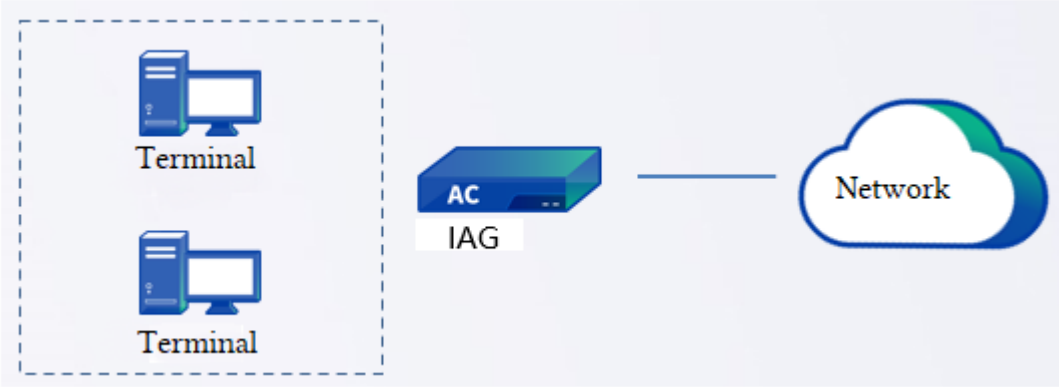
4.1 Configuration Steps:

1. Create new access check/control rules and configure specific inspection items or control items.

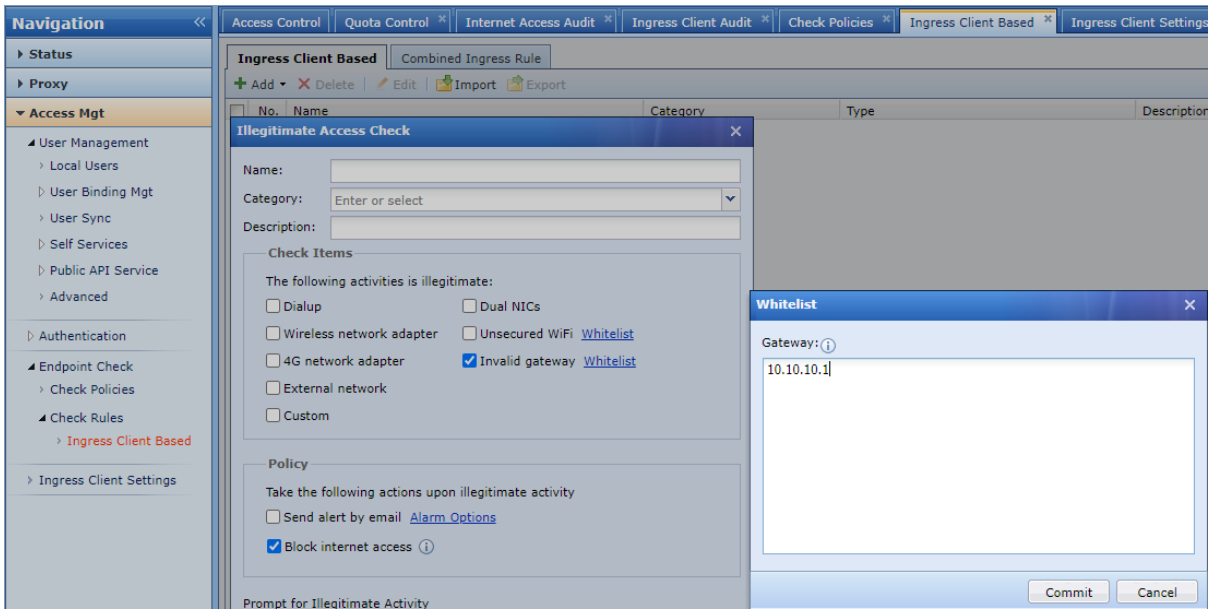
2. Configure endpoint check policy, refer to the previously configured rules, and select the applicable users.

4.2 Configuration Case:

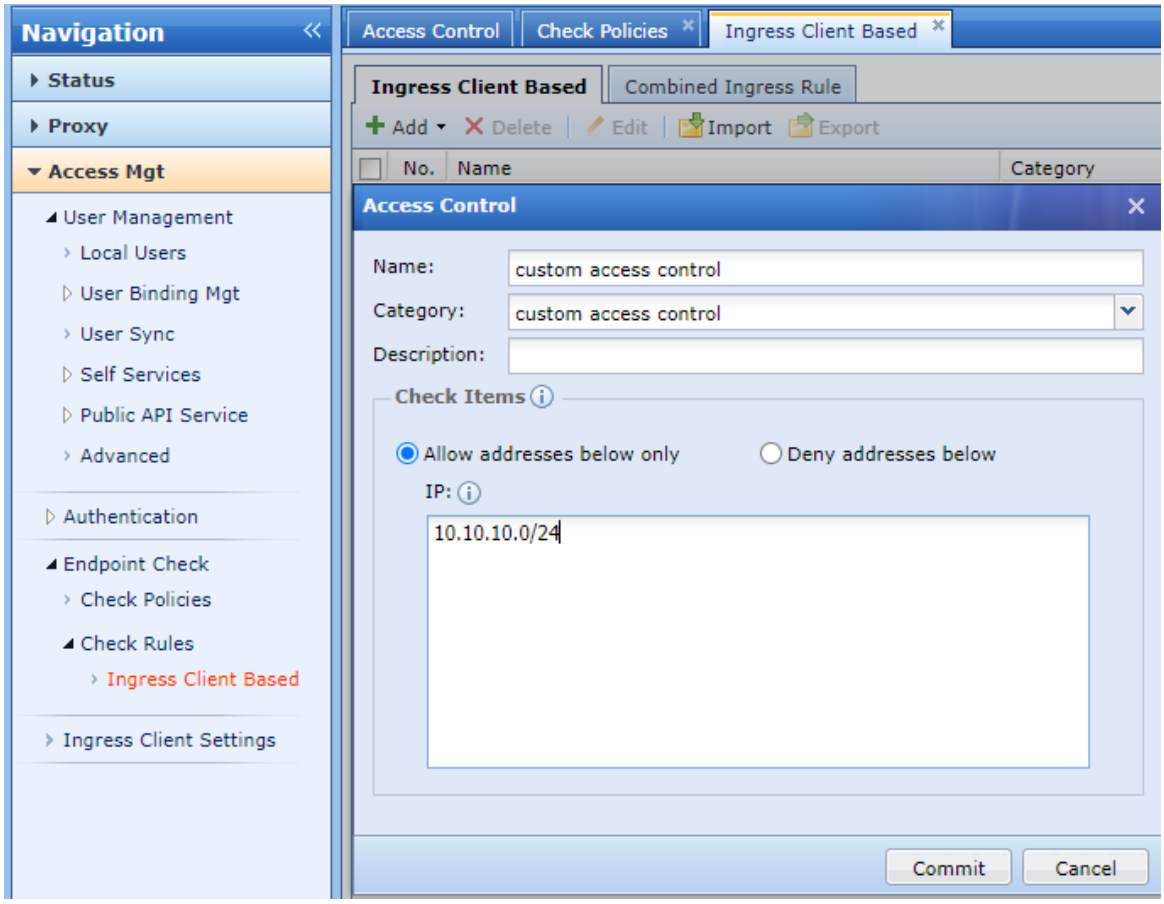
The customer private network deploys an IAG. The gateway of the terminal is required to be 10.10.10.1. When there are other gateways, the network will be disconnected. The address segment that can be accessed at the same time can only be 10.10.10.0/24.



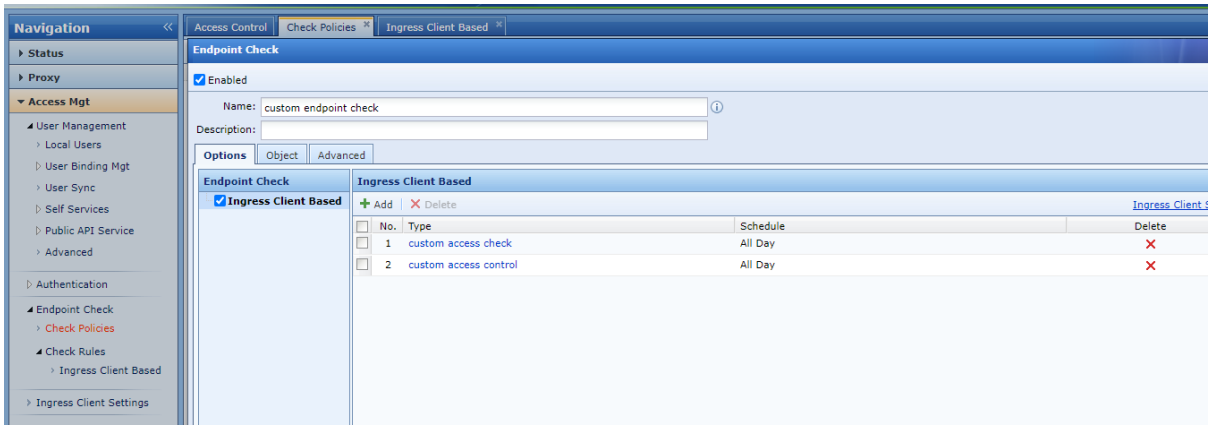
Create a new access check rule, tick invalid gateway, and fill in 10.10.10.1 in the whitelist.



Create a new access control rule, and only allow access to the section 10.10.10.0/24.



Create a new endpoint check policy, add the previously built access check and control rules, and select applicable users.



Chapter 5 Precautions

1. The terminal can only obtain the policy after passing the authentication, and the ingress client must be installed for the access check and control functions.

2. There must be no NAT in the path from the terminal to the IAG device. If there is NAT, the access check and control function will not take effect.

3. XP system without WFP module does not support access control function.

4. Combined ingress rules do not apply access check and control rules (combined ingress rules are for old ingress rules such as process and file based rule).

5. The ingress installed through MSI cannot prevent uninstallation. If you want to prevent uninstallation, you need to install the ingress in exe format, and enable the uninstall prevention function in the ingress client settings, and the terminal needs to obtain an endpoint check policy once. (You can download the ingress by popping up the ingress installation page by configuring the endpoint check policy, or you can download via http://IP:817/singress.exe directly on the device).

6. When the network is disconnected, all physical network cards will be disabled. After re-enabling, there will be 40s to detect whether there are violations. If there are violations, continue to disable the network card. When there is no violation, it will no longer be prohibited. If the policy is updated, it will also be updated within 40s.