Configuring application-based security policies to block WeChat

Security 周天 2020-12-25 Published

Network Topology

An overseas office needs to configure an application-based security policy to block YouTube. Since t here are no access conditions for youtube in China, the following is an experience case of configuring an application-based security policy to block WeChat.

The configuration method of blocking youtube and blocking WeChat is the same, the difference is that the classification of the application is different, you can find this application by searching youtube in the application search box.

The following matrix shows the hardware and software versions to which this configuration guide is a pplicable:

Hardware	Software version
F5030-D, F5060-D, F5080-D, F5000-AK515, F5000-AK525	E9620 or newer version
F5030, F5030-6GW, F5060, F5080, F5000-M, F5000-A, F5000-AI-20, F5000-AI-40, F5000-V30	E9628 or newer version
F5010, F5020-GM, F5020, F5040, F5000-C, F5000-S	E9342 or newer version
F1000-AI-20, F1000-AI-30, F1000-AI-50	E9345 or newer version
F1000-AI-60, F1000-AI-70, F1000-AI-80, F1000-AI-90	E8601 or newer version
F1005, F1010, F1003-L, F1005-L	E9536 or newer version
F1020, F1020-GM, F1030, F1030-GM, F1050, F1060, F1070, F 1070-GM, F1080, F1000-V70	E9345 or newer version

Restrictions and guidelines

When you configure a security policy, follow these restrictions and guidelines:

·Update the APR signature library to the latest version.

V7-APR-1.0.110 or newer version

·For the applications in a security policy to be identified, you must allow the dependent protocols of th e applications to pass through.

Configuration Steps

Analysis

·This security policy **p** can prohibit prohibit users from using WeChat.

·Configure security policy **pass** to allow common protocols for APR to identify applications correctly.

·Configure the security policies in the following order:

a. p

b. pass

Procedure

1. Assign IP addresses to interfaces and add the interfaces to security zones.

On the top navigation bar, click Network.

From the navigation pane, select Interface Configuration > Interfaces.

Click the Edit icon for GE 1/0/1.

In the dialog box that opens, configure the interface:

a. On the IPv4 Address tab, enter the IP address and mask of the interface. In this example, enter 2.2.2.1/24.

b. Click **OK**.

Configure the IP addresses of GE 1/0/2, in the same way you configure GE 1/0/1.

2. Configure security zones.

On the top navigation bar, click Network.

From the navigation pane, click Security Zones.

Click the Edit icon for security zone **Untrust**.

In the dialog box that opens, add GE 1/0/1 to the security zone.

Click the Edit icon for security zone **Trust**.

In the dialog box that opens, add GE 1/0/2 to the security zone.

3. Configure application groups.

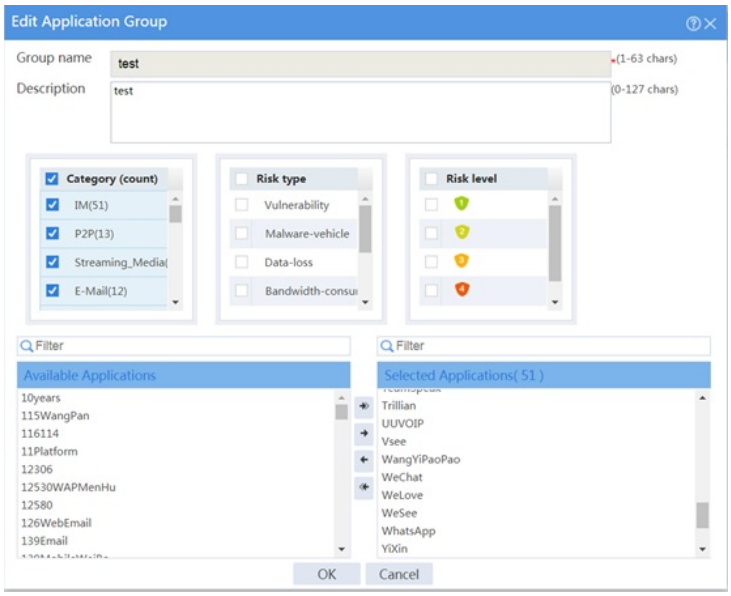
On the top navigation bar, click Objects.

From the navigation pane, select APP Security > APP Recognition > Application Groups.

Click Create.

In the dialog box that opens, configure an application group named test:

¡ Enter group name test.
¡ Add wechat applications in the **IM** category to the **Selected Applications** pane.
¡ Click **OK**.



4. Configure a security policy named **pass**.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create**.

In the dialog box that appears, configure the security policy:

¡ Enter policy name **pass**.
¡ Select source zone **Any**.
¡ Select destination zones **Any**.
¡ Select policy type **IPv4**.
¡ Select action **Permit**.

Click **OK**.

5. Configure a security policy named **p**.

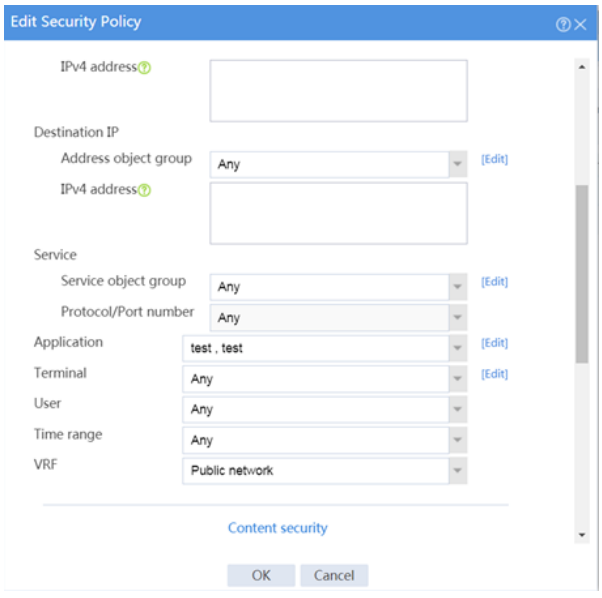
On the top navigation bar, click **Policies**.

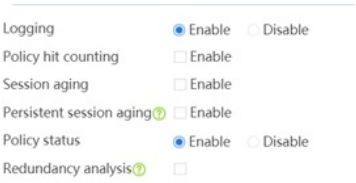
From the navigation pane, select **Security Policies** > **Security Policies**.

Click **Create**.

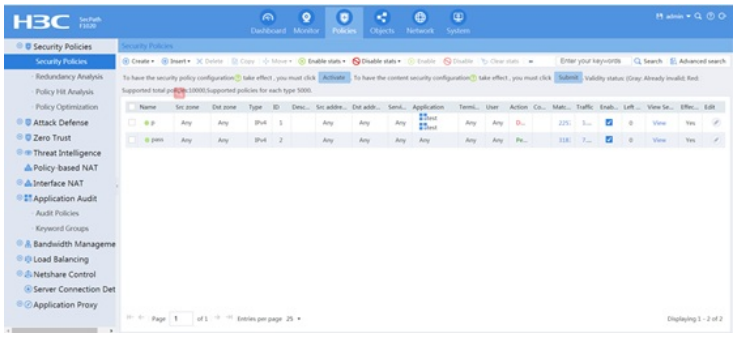
In the dialog box that appears, configure the security policy:

¡ Enter policy name **p**.
¡ Select source zone **Any**.
¡ Select destination zones **Any**.
¡ Select policy type **IPv4**.
¡ Select action **Deny**.
¡ Select application group **test**.
¡ Select logging **Enable**.





Click **OK**.



6. Configure an audit policy named **test**.

On the top navigation bar, click **Policies**.

From the navigation pane, select **Application Audit** > **Audit Policies**.

Click **Create**.

In the dialog box that appears, configure the application audit policy:

¡ Enter policy name **test**.

¡ Select source zone **Any**.

¡ Select destination zones **Any**.

¡ Select policy type **Audit**.

Configure an **audit rule** to perform refined auditing on the behaviors and behavior contents of appli cations. This item can be configured only for an Audit-type policy.

¡ Click **Create**.

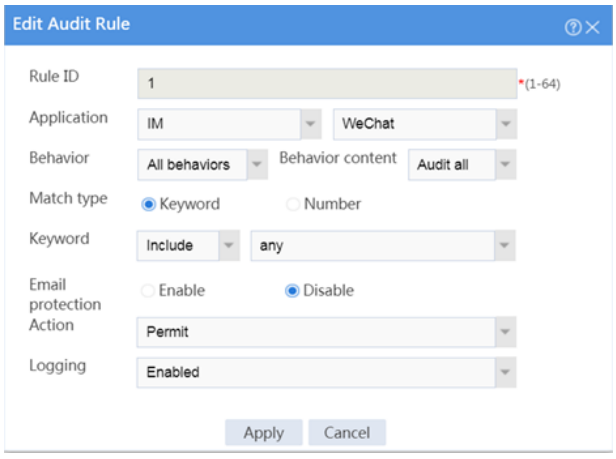
¡ Enter rule ID **1**.

¡ Select application **IM** > **WeChat**.

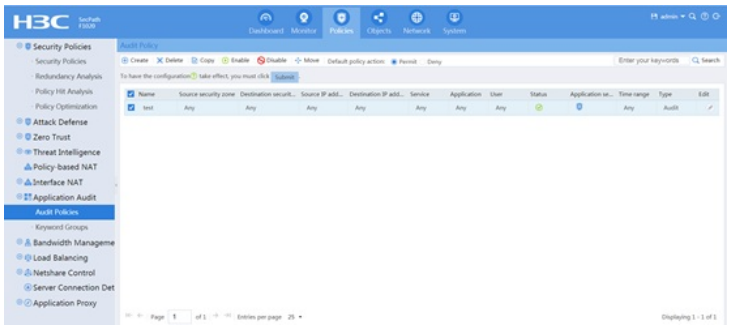
¡ Select behavior **All behaviors**.

¡ Select behavior content **Audit all**.

¡ Select logging **Enabled**.



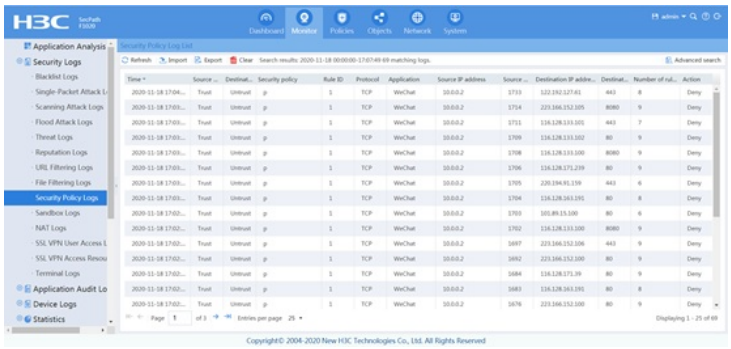
Click **Apply**.



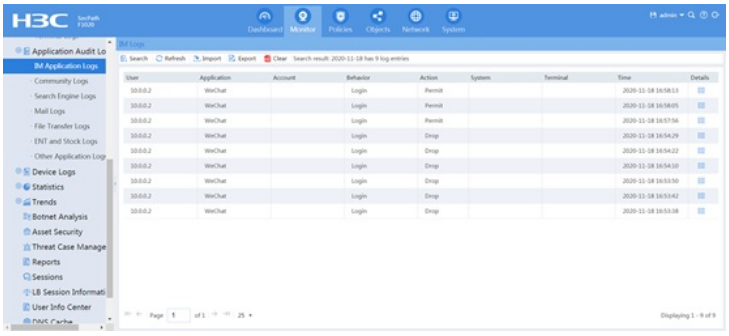
Verifying the configuration

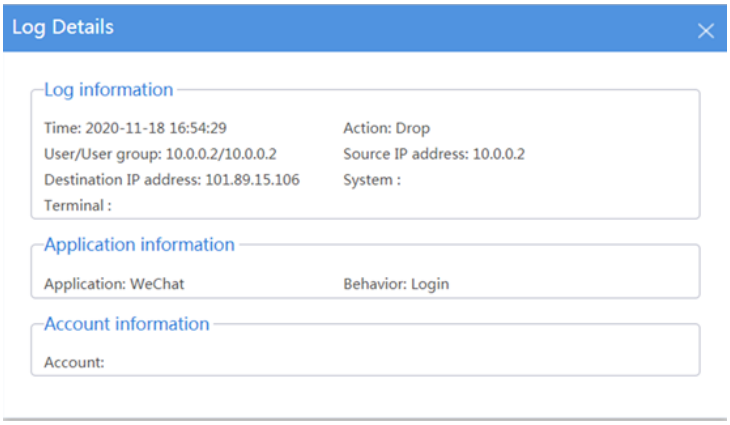
Verify that the users can not use WeChat, open WeChat cannot display QR codes, and can not log on by scanning QR codes.

Verify that security polices can be hit correctly by selecting **Monitor** > **Security Logs** > **Security Policy Logs**. The following are examples of security policy hitting:



Verify that application audit policy can be hit correctly by selecting **Monitor** > **Application Audit Log** > **IM Application Logs**. The following are examples of application audit policy:





Key Configuration

Summary

In addition to configuring security policies, application audit policies must also be configured.

The configuration method of blocking youtube and blocking WeChat is the same, the difference is that the classification of the application is different, you can find this application by searching youtube in the application search box.