H3C SecPath UTM Series Anti-Spam Configuration Example

Keywords: Anti-spam, SMTP, POP3

Abstract: This document presents an anti-spam configuration example for UTM devices.

Acronyms:

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Full spelling</th>
</tr>
</thead>
<tbody>
<tr>
<td>UTM</td>
<td>Unified Threat Management</td>
</tr>
<tr>
<td>SMTP</td>
<td>Simple Mail Transfer Protocol</td>
</tr>
<tr>
<td>POP3</td>
<td>Post Office Protocol, Version 3</td>
</tr>
</tbody>
</table>
Table of Contents

Feature Overview ........................................................................................................................................... 3
Application Scenarios .................................................................................................................................. 3
Configuration Guidelines ............................................................................................................................ 3
Anti-Spam Configuration Example ............................................................................................................ 3
  Network Requirements ............................................................................................................................... 3
  Configuration Considerations .................................................................................................................... 4
  Hardware/Software Version Used ............................................................................................................. 4
  Configuration Procedures ........................................................................................................................ 4
    Basic Configuration ................................................................................................................................ 4
    Anti-Spam Configuration ......................................................................................................................... 7
  Verification ............................................................................................................................................... 10
Related Documentation ............................................................................................................................... 11
Feature Overview

By cooperating with a Commtouch mail server (a third-party mail server), the anti-spam feature of an H3C UTM device can inspect all emails sent from external networks to the internal network and process the emails as configured, so as to prevent spam from wasting the resources of the internal network.

With the anti-spam feature configured, the device forwards all emails received from external networks to the Commtouch mail server for inspection and, after receiving the inspection results, processes the emails based on the actions specified in the anti-spam policy.

The anti-spam feature supports inspecting Simple Mail Transfer Protocol (SMTP) emails and Post Office Protocol, Version 3 (POP3) emails:

- **SMTP**: In a scenario where the SMTP clients are on the external network and the SMTP server is on the internal network.
- **POP3**: In a scenario where the POP3 clients are on the internal network and the POP3 server is on the external network.

Application Scenarios

The anti-spam feature can be deployed to check emails entering an internal network to prevent email spam from occupying resources of the internal network.

Configuration Guidelines

Before configuring the anti-spam feature, ensure that:

- The device can communicate with the Commtouch mail server normally. The address of the Commtouch mail server is http://resolver%d.h3c.ctmail.com, where %d indicates a number in the range from 1 to 10.
- The device has a legal, effective license of the anti-spam feature.
- The device can connect to http://www.h3c.com to verify the validity of the license for the anti-spam feature. When the license of the anti-spam feature expires, all anti-spam configurations will not be effective any more.

Anti-Spam Configuration Example

Network Requirements

As shown in Figure 1, the internal network of a company is 4.1.1.0/24, and the external network is 192.168.100.0/22. Configure the UTM device to inspect emails received from the POP3 server and process those emails as follows:

- Modify the subjects of emails from known spam sources and log them.
- Modify the subjects of emails from unknown spam sources and log them.
- Log suspicious emails.
- Forward normal emails normally.
Figure 1 Network diagram for anti-spam configuration

Configuration Considerations

- Redirect the traffic of interest for in-depth inspection.
- Configure the anti-spam policy and rules.
- Apply the policy to the segment.

Hardware/Software Version Used

```bash
<H3C>dis ver
H3C Comware Platform Software
Comware Software, Version 5.20, Ess 5115
Copyright (c) 2004-2009 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
H3C SecPath U200-CM uptime is 0 week, 3 days, 20 hours, 54 minutes

CPU type: RMI XLS404 800MHz CPU
512M bytes DDR2 SDRAM Memory
32M bytes Flash Memory
247M bytes CF0 Card
PCB   Version:Ver.B
Logic  Version:  2.0
Basic BootWare Version: 1.23
Extend BootWare Version: 1.23

[FIXED PORT] CON       (Hardware)Ver.B, (Driver)1.0,    (Cpld)2.0
[FIXED PORT] GE0/0     (Hardware)Ver.B, (Driver)1.0,    (Cpld)2.0
[FIXED PORT] GE0/1     (Hardware)Ver.B, (Driver)1.0,    (Cpld)2.0
[FIXED PORT] GE0/2     (Hardware)Ver.B, (Driver)1.0,    (Cpld)2.0
[FIXED PORT] GE0/3     (Hardware)Ver.B, (Driver)1.0,    (Cpld)2.0
[FIXED PORT] GE0/4     (Hardware)Ver.B, (Driver)1.0,    (Cpld)2.0
[SUBCARD  1] 2GE       (Hardware)Ver.B, (Driver)1.0,    (Cpld)1.0
```

Configuration Procedures

Basic Configuration

Configuring interface GE 0/1

Select Device Management > Interface from the navigation tree and then click the icon of GE 0/1 to enter the interface configuration page. Perform the configurations shown in the following figure and click Apply.
Select **Device Management > Zone** from the navigation tree and then click the icon of the Untrust zone to enter the page for modifying the security zone configurations. Add interface GE 0/1 to the Untrust zone as shown in the following figure, and click **Apply** to complete the operation and return to the security zone page.

**Configuring interface GE 0/4**

Similarly, assign IP address 4.1.1.1/24 to interface GE 0/4 and add the interface to security zone Trust. Selecting **Device Management > Interface** from the navigation tree, you should see the following list:
Configuring NAT

To enable internal hosts to connect to the external network through the UTM device, you need to configure a NAT policy on interface GE 0/1. In this example, the policy references ACL 3004 and uses the NAT mode of Easy IP.

Select Firewall > ACL from the navigation tree and then create ACL 3004 and add a rule to the ACL to identify the flow of interest. In this example, the ACL permits packets sourced from 4.1.1.0/24. The configurations are shown in the following figure:

Configuring a route

Select Network > Routing Management > Static Routing from the navigation tree and configure a default route, setting the next hop to the IP address for the intranet side interface of the router that connects the GE 0/1 interface of the UTM device with the external network (192.168.100.254 in this example).
Configuring a redirect policy

Configure a redirect policy to redirect the flow of interest to the i-Ware platform for in-depth analysis. In this example, traffic between zone Trust and zone Untrust that matches ACL 3000 will be redirected to segment 0.

First, select Firewall > ACL from the navigation tree and then create ACL 3000 and add rules to the ACL to identify the traffic of interest. The configurations are shown in the following figure:

Then, select IPS | AV | Application Control > Advanced Configuration from the navigation tree and create a redirect policy to redirect traffic matching ACL 3000 to segment 0.

Anti-Spam Configuration

Select IPS | AV | Application Control > Advanced Configuration from the navigation tree and click the Application Security Policy link to enter the in-depth inspection configuration page.

Enabling anti-spam inspection

Select Anti-Spam > Anti-Spam from the navigation tree and perform the following configurations in the Server Configuration area:

- Select the Antispam inspection check box.
- Click Apply.
- After a while, you will see that the operation status becomes normal.
If the UTM device connects to the Commtouch mail server through a proxy server, you need to configure the proxy server according to the networking scheme.

The anti-spam signature database stores all email spam signatures that the device can identify. The license of the anti-spam feature has a validity period specified. After the license expires, you need to recharge to obtain a new license before upgrading the anti-spam signature database.

Creating and applying the anti-spam policy

Under Policy Application List, click Add and perform the following configurations:

- Type test as the name.
- Select Modify subject and log as the action for POP3 emails from known spam sources.
- Select Modify subject and log as the action for POP3 emails from unknown spam sources.
- Select Log as the action for suspicious POP3 emails.
- Select Log as the action for normal POP3 emails.
Under **Apply Policy**, click **Add** and perform the following configurations on the page that appears:

- Select segment 0.
- Click **Apply**.

Now, segment 0 should appear on the list under **Apply Policy**. Click **Apply** to complete the operation.
Activating configurations

After the application operation is complete, the anti-spam configuration page appears again, as shown in the following figure. Click **Activate** and confirm your operation.

Verification

On internal host 4.1.1.2, configure Outlook Express to receive emails. Then, on the web interface of the device, select **Log Management > Anti-Spam Logs** from the navigation tree. Logs about inspection and processing of emails destined for the user should appear on the list.
### Related Documentation

*Anti-Spam Configuration* of the Web configuration manual.