

CheckPoint Software Technologies LTD. ä

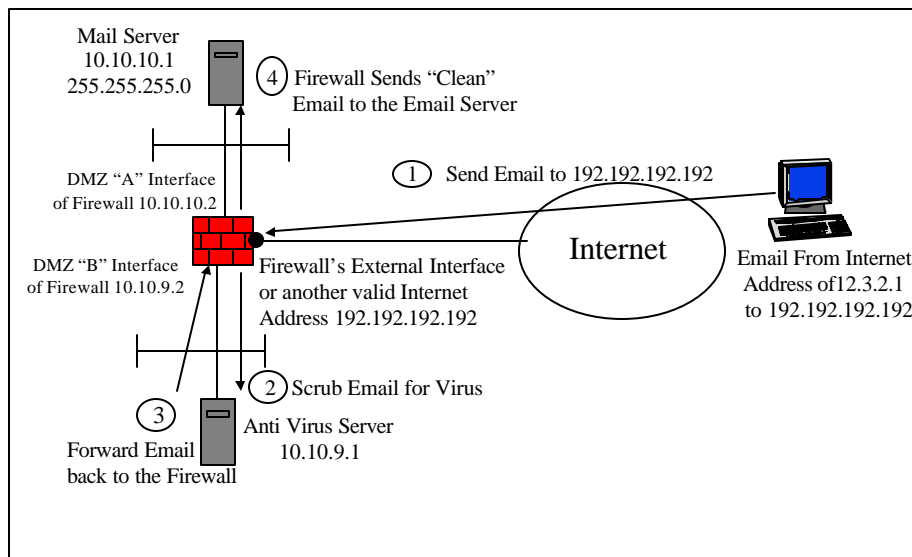
FireWall-1 ä Version 3.0B
Patch Level 3064
SMTP Security Server
Quick Reference

Authored By: Joe DiPietro
CheckPoint Software Technologies LTD. ä
Date Published: April 9, 1998

How to Setup the SMTP Resource

The Following Diagram shows the general process for the SMTP Security Server Resource within Firewall-1 version 3.0B. If you don't already have patch 3064, please contact the reseller that you purchased Firewall-1 from and obtain this patch. From this Diagram, we will configure the components necessary to use the SMTP Security Server to Scrub Email's for Viruses and to forward them to the appropriate Mail Server after they have been cleaned. This document assumes you are familiar with Firewall-1. If not, please read the documentation that came with your CDROM, and other reference guides located at: <http://www.checkpoint.com/~joe>

SMTP Email Process



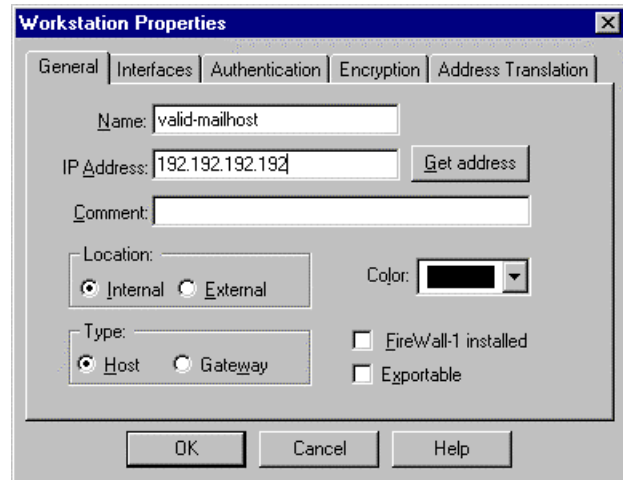
Note: If you use another valid Internet Address, make sure to configure the firewall for "Proxy -ARP" for that IP Address. This is described in detail within the "Address Translation Guide" for version 3.0 under <http://www.checkpoint.com/~joe>.

Steps to configure the SMTP Resource

1. Define an object with the Valid Internet Address of the Mail Server so people can send email's to this IP Address (192.192.192.192)
2. Define an object for the IP Address of the Mail Server (this assumes it is different from above. (10.10.10.1)
3. Define the object for the Anti Virus Server (10.10.9.1)
4. Define the "service" for the Anti Virus Server
5. Define the SMTP Resource
6. Define the Rule with the SMTP Resource to allow Email's to be "cleaned" for Viruses
7. Validate the Email Transfer works properly
8. Troubleshoot if necessary

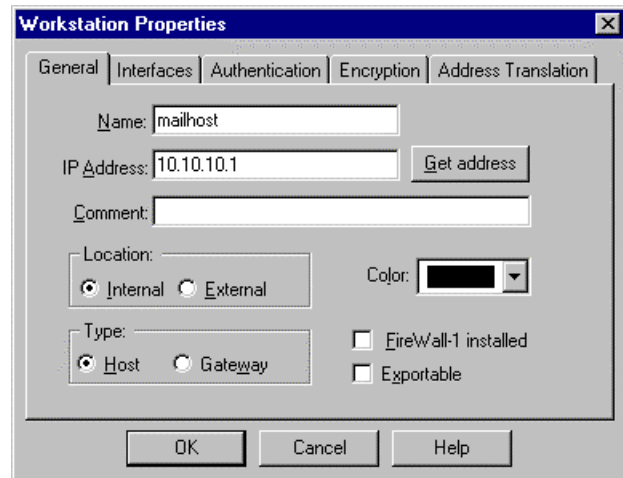
1. Define the network object of the valid address of the mail server to the Internet. This could be the outside interface of the Firewall as well.

Manage → Network Objects → New → Workstation



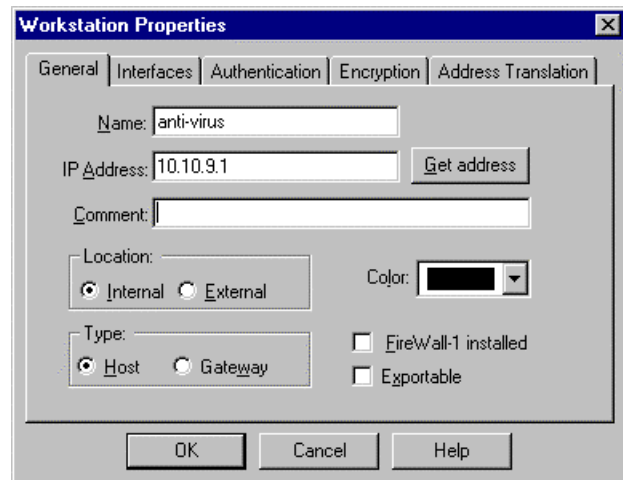
2. Define the network object of the Mail Server as follows:

Manage → Network Objects → New → Workstation



3. Define the network object of the Anti-Virus Server as follows:

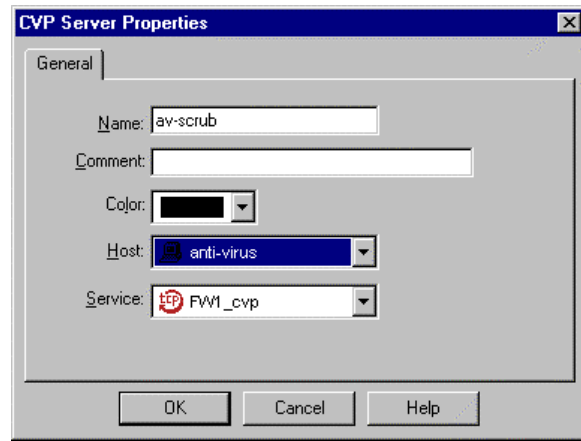
Manage → Network Objects → New → Workstation



4. Define the Anti-Virus Service

Manage → Servers → New → CVP

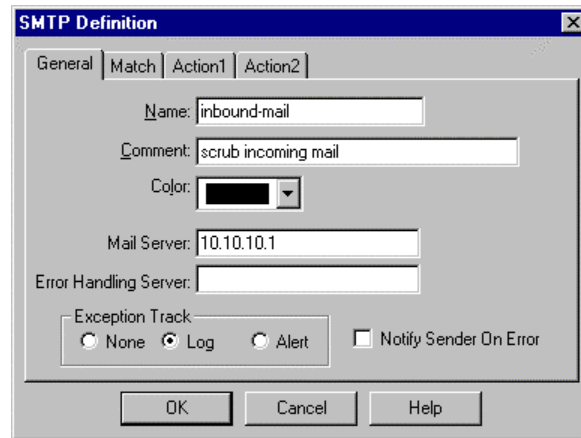
Name = av-scrub
 Host = anti-virus
 Service = FW1_cvp



5. Define the SMTP Resource as follows:

Manage → Resources → New → SMTP

Name = inbound-mail
 Mail Server = 10.10.10.1
 Exception Track = log

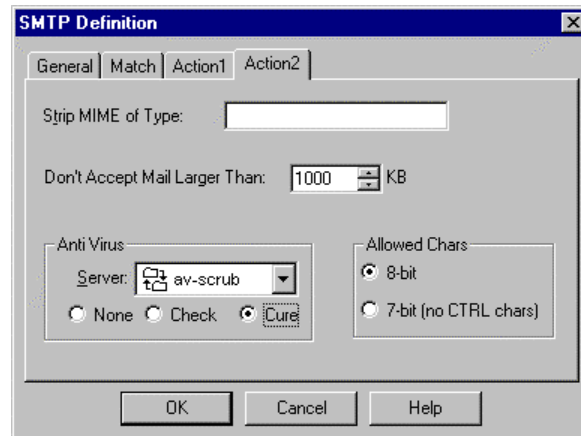


Now Select the "Action 2" Tab

Select the previously defined av-scrub as the Anti Virus Server

And "Cure" viruses

Click OK



6. Now Write the appropriate rulebase to allow the SMTP to be forwarded and scrubbed by the antivirus server...

No.	Source	Destination	Service	Action	Track	Install On	Time	Con
1	Any	valid-mailhost	smtp->inbound-mail	accept	Long	Gateways	Any	
2	Any	Any	Any	drop	Long	Gateways	Any	

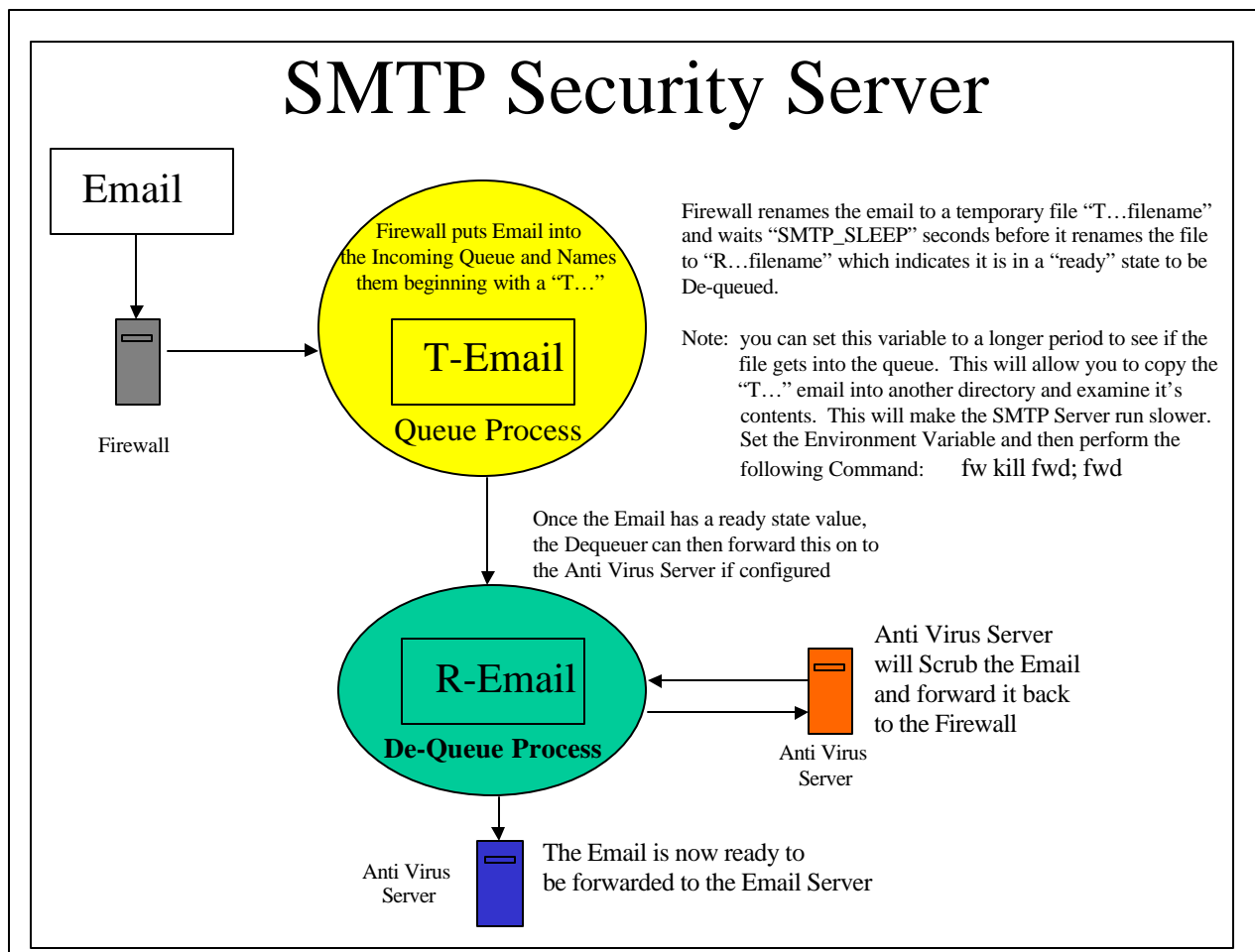
Select the destination of the valid-mailhost, with the service of SMTP with the resource of inbound-mail, and the action of Accept.

7. Validate the above configuration works by looking in the Log files to validate that the SMTP is being accepted and forwarded on to the Anti Virus machine and then to the Email Server.

Trouble Shooting

The Overview of the SMTP Security Server is shown below. If you have a problem, there are three places where the system may not be working. They are the following:

1. Connection between the Email Client and the Firewall SMTP Security Server
2. Connection between the Firewall Mail Dequeueer and the Anti Virus Server
3. Connection between the Firewall Mail Dequeueer and the Final Email Server



Troubleshooting Step 1.

1. Always look in the log file to see if the email connection is accepted from the appropriate rule in the rulebase. In our case, rule number 1 should have accepted the SMTP Connection to the Valid-Mailhost. Also check the "Info" portion of the log file. This is where the connection is described in more details.
2. Make sure the email has completed the queuing process and has a name of "T..." under the spool directory. This should be located under the default installation directory of:

Windows NT = \winnt\fw\spool

Unix = /etc/fw/spool

3. If there is no file in this directory after the email has been sent by the client, and the log file tells us that the SMTP Connection has been accepted, make sure the SMTP Security Server has been configured. Validate this by running the following:

Windows NT = \winnt\fw\bin\fwconfig

Unix = /etc/fw/bin/fwconfig

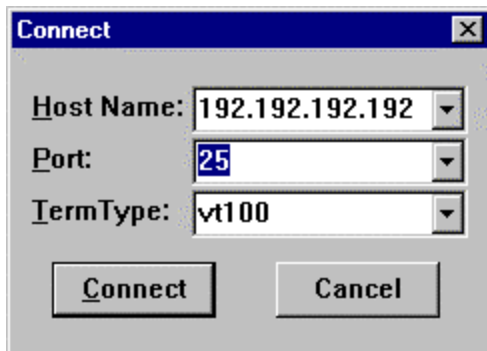
Make sure the SMTP Security Server is "checked" to start with the other Firewall Security Servers. This will place a "asmtpd" entry into the \winnt\fw\conf\fwauthd.conf file as follows (Unx = /etc/fw/conf/fwauthd.conf)

```
C:\WINNT\FW\conf>type fwauthd.conf
259  aclientd  wait  259
23   atelnetd  wait  0
21   aftp      wait  0
80   ahttpd     wait  0
513  arlogind  wait  0
25   asmtpd    wait  0
10081 lhttpd     wait  0
C:\WINNT\FW\conf>
```

4. Run telnet to the Valid-Mailhost on port 25 to see if the SMTP Security Server works OK.

On Windows 95/NT use the telnet client as follows:

On Unix type in the following:



```
telnet 192.192.192.192 25
```

Enter the command "help" or "?" to see FW-1 smtp server replies.

5. Some additional tracing info may be in your \winnt\fw\log\asmtpd.log or /etc/fw/log/asmtpd.log.

Troubleshooting Step 2.

1. Make sure the firewall can ping the Anti Virus server for connectivity.
2. If this is successful, then see if the Anti Virus software has received an email from the Firewall. This will tell you if the Firewall has accepted the email from the client, queued it, renamed the email and forwarded this on to the Anti Virus Server.
3. Validate that the Proper CVP ports are configured on the Anti Virus Machine and the Firewall Resource. This is done in Step 4 above. By Default the FW1_cvp is using port 18181.
4. Use a packet sniffer, or the "Snoop" command in Unix or the Network Monitor Agent in NT to see if the Firewall dequeuer has any communication with the Anti Virus Machine.

Troubleshooting Step 3.

1. Make sure you can ping the final Email Server
2. Try and use the SMTP Resource without the Anti Virus Server defined in the configuration step 5B above. Now download the Security Policy to the firewall again and see if the Email will pass from the Queuer to the Dequeuer and then on to the Email Server. If this is OK, then the process is not working correctly in step 2.
3. Try and telnet from the firewall to the final Email Server on port 25 to see if you can make a connection. This will tell you if the SMTP process on the Email Server is configured and active, so that the Dequeuer can forward the emails to the Email Server.