CONTENTS

Support Site: http://www.cisco.com/en/US/products/ps11169/serv_group_home.html

If you purchased support through a reseller or another

Configuration Changes

You can make configuration changes while email operations proceed normally.

Commit or Abandoning Changes

You must explicitly save most configuration changes.

Change the Admin Password

CHAPTER

Bounce Limits

You use the Network > Bounce Profiles page (or the `bounceconfig`apo.53.1(u c.65(ra)-5(e.65(ap)-te bo6 Tw (w.4(e1.8735f108

Directory Harvest Attack Prevention: Drop Connection if DHAP threshold is

Step 7 Submit and commit your changes.

Related Topics

- Sender Verification: Host, page 7-26
- Sender Verification: Envelope Sender, page 7-26
- Implementing Sender Verification — Example Settings, page 7-28
- Testing Your Settings for Messages from Unverified Senders, page 7-33
- Sender Verification and Logging, page 7-35

Step 5 Submit and commit your changes.

Searching for Addresses within the Sender Verification Exception Table

Procedure

Step 1 Enter the email address in the Find Domain Exception section of the Exception Table page.

Step 2 Click **Find**.

CHAPTER

Step 2 Choose the listener to edit in the Overview for Listener field.

Step 3 Click **Export RAT.**

Step 4

CHAPTER 9

Using Message Filters to Enforce Email Policies

The Cisco appliance contains extensive content scanning and message filtering technology that allows you to enforce corporate policies and act on specific messages as they enter or leave your corporate

the total score. If you set the threshold value for the message filter to 6, AsyncOS would determine that the threshold score has been met. Or, if the message contained one instance of each term, the total value would be 6, and this score would trigger the filter action.

AND Test and OR Tests in Message Filters

When evaluating AND or OR tests within message fi

Attachment File[a]

For more information, see Chapter 20, “S/MIME Security Services.”

S/MIME Gateway Verified Rule

Add Heading `add-heading(`

Table 9-6 Attachment Groups (continued)

Attachment Group Name	Scanned File Types
Text	• txt • html • xml
Image	• bmp • cur • gif • ico • jpeg • pcx • png • psd • psp • tga • tiff
Media	• aac • aiff • asf • avi • flash • midi • mov • mp3 • mpeg • ogg • ram • snd • wav • wma • wmv

Related Topics

-

When flagged for quarantine, the message continues through the rest of the email pipeline. When the message reaches the end of the pipeline, if the message has been flagged for one or more quarantines then it enters those queues. Otherwise, it is delivered. Note that if the message

Image Analysis

Dropping Attachments by Dictionary Matches

This

CHAPTER

Defining Senders and Recipients for Mail Policies

You can define senders and recipients to whom the policy applies in the following ways:

- Full email address: `user@example.com`
- Partial email address: `user@`

CHAPTER

Subject Header

Subject Header: Does the subject header match a certain pattern?

Contains terms in content dictionary: Does the subject header contain

Related Topics

Notes on Configuring Content Filters in the GUI

-

  - Western European/Latin-1 (ISO 8859-1)
  - Western European/Latin-1 (Windows CP1252)
  - Traditional Chinese (Big 5)
  - Simplified Chinese (GB 2312)
  - Simplified Chinese (HZ GB 2312)
  - Korean (ISO 2022-KR)
  - Korean (KS-C-5601/EUC-KR)
  - Japanese (Shift-JIS (X0123))
  - Japanese (ISO-2022-JP)
  - Japanese (EUC)

  You can mix and match multiple character sets within a single content filter. Refer to your web browser's documentation for help displaying and entering text in multiple character encodings. Most browsers can render multiple character sets simultaneously.

- On the Incoming or Outgoing Content Filters summary pages, use the links for "Description," "Rules," and "Policies" to change the

CHAPTER

Heuristics

The default text is:

For each mail policy, you can specify thresholds for some of the categories, and determine the action to

Cisco Anti-Spam: an Overview

Configuring IronPort Anti-Spam Scanning

After the system is set up, you can configure the an

Figure 13-4 Mail Relayed by MX/MTA — Simple

Related Topics

- Testing Anti-Spam Configuration: Example Using SMTP, page 13-25

Testing Anti-Spam Configuration: Example Using SMTP

For this example, the mail policy must be configured to receiv and1.he.eam

-

End-User Safelist

If the end users in your organization have configured Safelist for their own email accounts, graymail messages from a sender in the safelist will not be

Step 3 Depending on your requirements, do the following:

-

CHAPTER

CHAPTER

-

CHAPTER

– Regular Expressions for Identifying Identification Numbers, page 18-15.

Content Matching Classifier Examples

The following examples show how classifiers match message content:

-

About Assessing Violation Severity

When the DLP scanning engine detects a potential DLP violation, it calculates a risk factor score that represents the likelihood that the

Step 2

Using LDAP to Identify Message Senders for Enterprise Manager

When the Email Security appliance sends DLP incident data to Enterprise Manager, the appliance must include the complete LDAP distinguished names in order to identify message senders. The appliance retrieves this information from an LDAP server.

Before You Begin

- Complete all steps to this point in the table in How to Set up Data Loss Prevention in Deployments

Lost Connectivity Between the Email Security Appliance and Enterprise Manager

If connectivity between the Email Security appliance and Enterprise Manger is lost, any data that the

Procedure

Step 1 Select

Step 8 Select **Encrypt and Deliver Now (Final Action)** from the **Add Action** list.

- Import an existing S/MIME certificate to the appliance. See Importing an S/MIME Signing Certificate, page 20-8.

Setting Up Public Keys for S/MIME Encryption

You must add the public key of the recipient's S/MIME certificate to the appliance for encrypting messages. Depending on your organizational policies and processes, you can use one of the following methods to add the public key to the appliance:

-

Step 4 Submit and commit your changes.

Note Use the `smimeconfig` command to create sending profiles using CLI.

Edit an S/MIME Sending Profile

Step 1 Click **Mail Policies** > **Sending Profiles**

CHAPTER

As messages are received on a listener used to send

How to Verify Incoming Messages Using DMARC

Step 8 Submit and commit your changes.

Edit a DMARC Verification Profile

Procedure

Step 1 Choose **Mail Policies** > **DMARC**.

Step 2 Click the intended verification profile name.

Step 3 Edit the intended fields as described in Create a DMARC Verification Profile, page 21-35.

Step 4 Submit and commit your changes.

CHAPTER 22

Text Resources

Example Dictionary Entries

Tai

CHAPTER

Related Topics

- Enabling TLS Connection Alerts, page 24-13

Enabling TLS Connection Alerts

Procedure

```
- LIMITS - Change the injection limits.

- SETUP - Configure general options.


 Configan[DAP tionsyano rerng e messagetions. Configan[DAP qutions.

 Configan[MTP autUP -s.[]>Tw( /F9/TT2 12.40698 594 Tm66.6tion)esa Gu(s.)BT/TT2 1-2.4069-5.5113 594
```

```
- NEW - Create a new listener.

- EDIT - Modify a listener.

- DELETE - Remove a listener.

- SETUP - Change global settings.

[]> edit


Enter the name or number of the listener you wish to edit.

[]> 1


Name: InboundMail

Type: Public

Interface: PublicNet (192.168.2.1/24) TCP Port 25

Protocol: SMTP

Default Domain:

Max Concurrency: 1.02 .e8  iw0w113 TDnEu

Domain Ma13 TDp: Disabled

TLS: No

r9 T48uth13 TDentication: Disabled

Bounce Profile: Default

Use SenderBase For Reputation Filters and IP Profiling: Yes

Footer: None

LDAP: Off


Choose th13 TDe operation you want to 13 TDperform:

- NAME - Change the name of the listener.

- INTERFACE - Change the interfac13 TDe.

- LIMITS - Change the injection limits.
```

Set Email Delivery Parameters

The `deliveryconfig` command sets parameters to be used when delivering email from the appliance. The appliance accepts email using multiple mail protocols: SMTP and QMQP. However, all outgoing

-

See Controlling Email Delivery Using Destination Controls, page 25-42 for information about the `destconfig` command and how Virtual Gateway addresses are affected.

When you create a "group," of Virtual Gateway addresses, the good neighbor table settings for Virtual Gateway are applied to the group, even if the group consists of 254 IP addresses.

For example, suppose you have created group of 254 outbound IP addresses set up as a group to cycle through in a "round-robin" fashion, and suppose the good neighbor table for

Exporting and Importing a Global Unsubscribe File

Our Email Gateway configuration now looks like this:

Figure 25-15 Global Unsubscribe Example

Review: Email Pipeline

CHAPTER 26U fSp

If you configure the LDAP servfile for load 9 Tbalancing, 9 Tthese connections are distributed 9 Tamong the

Figure 26-4 Enabling Acceptance and Routing Queries on a Listener

Enabling LDAP Queries on a Private Listener

In this example, the private listen

Specific permissions must be made to a Microsoft Exchange 2000 server in order to allow “anonymous” or “anonymous bind” authentication for the purpose of querying user email addresses. This can be very useful when an LDAP query is used to determine th

–

Note that a server may be unreac

- Outgoing SMTP Authentication, page 26-40
-

Figure 26-13 Selecting an SMTP Authentication Profile via the Edit Listener page

Once a listener is configured to use the profile, the Host Access Table default settings can be changed so that the listener allows, disallows, or requires SMTP Authentication:

Figure 26-14 Enabling SMTP Authentication on a Mail Flow Policy

Related Topics

- SMTP Authentication and HAT Policy Settings, page 26-37
-

Table 26-9

-

CHAPTER

- Use the SenderBase Reputation service to drill down on and examine the relationship between specific IP addresses, domains, and organizations to obtain more information about a sender.
- Drill down on specific senders to obtain more information about a sender from the SenderBase Reputation Service, including a sender's SenderBase Reputation Score and which sender group the

The Sender Profile pages displayed for IP addresses, network owners, and domains vary slightly. For each, the page contains a graph and summary table for incoming mail from this sender. Below the graph is a table listing domains or IP addresses associated with the sender (the Sender Profile page for individual IP addresses does not contain the detailed listing) and an information section with the current SenderBase, sender group, and network information for the sender.

-

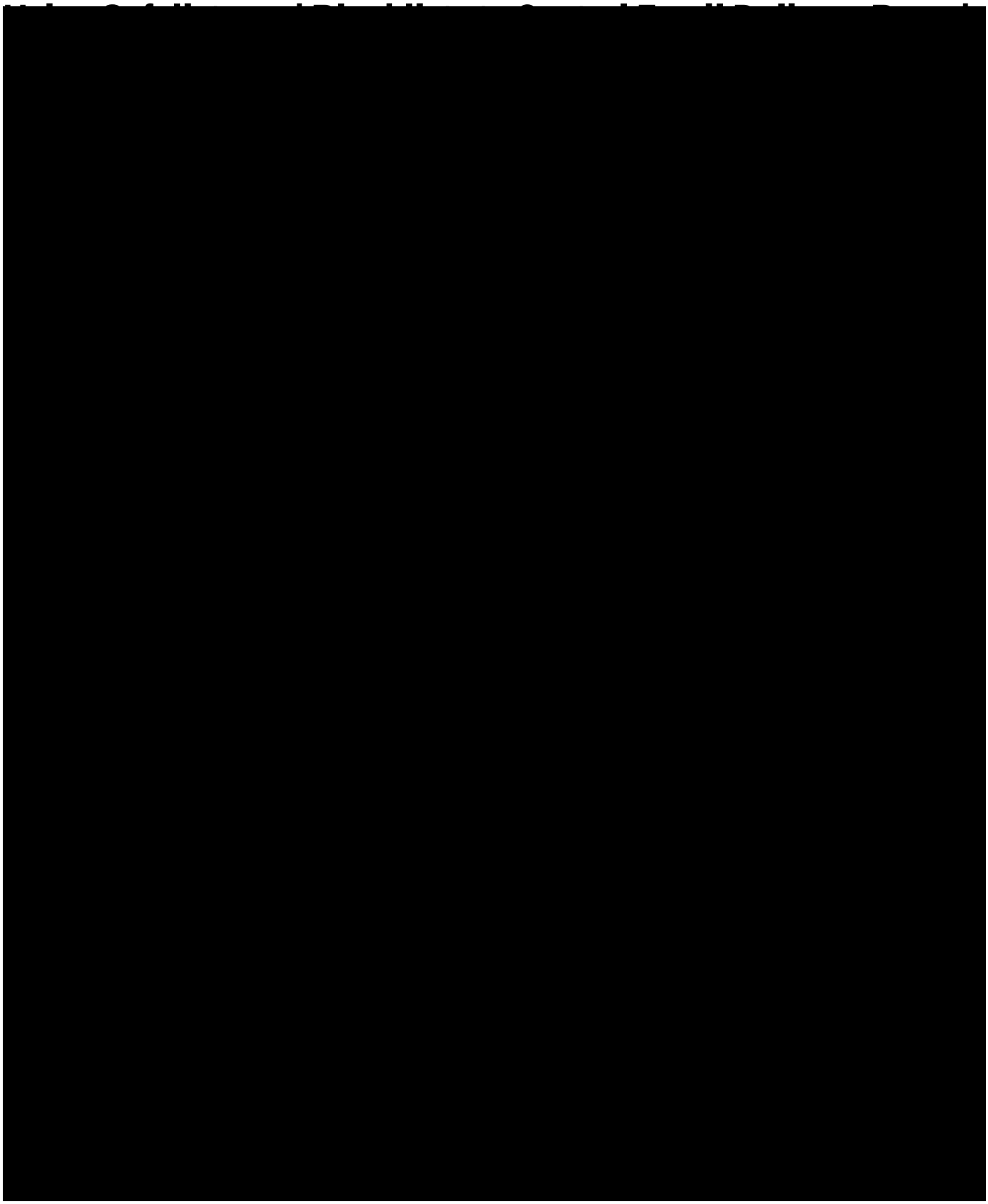
- Compromised user accounts that might be used to send spam in bulk.
- Out-of-control applications in your organization that use email for notifications, alerts, automated statements, etc.
- Sources of heavy email activity in your organization, for internal billing or resource-management purposes.
- Sources of large-volume inbound email traffic that might not otherwise be considered spam.

Note that other reports that include statistics for internal senders (such as Internal Users or Outgoing Senders) measure only the number of messages sent; they do not identify senders of a few messages to a large number of recipients.

- See also Effects of Time Adjustments on Retention Time, page 30-4.

CHAPTER

Enabling and Configuring the Spam Quarantine



- The Trace debugging tool.
- Spam, policy, virus, and outbreak quarantines.
- Cisco Email Encryption profiles.

After defining the access levels for a custom user role, you need to assign the specific mail policies, content filters, DLP policies, quarantines, or encryption profiles for which the delegated administrators will be responsible.

For example, you can create two different DLP policy administrator roles that are responsible for different RSA Email DLP policies. One role is only responsible for DLP violations related to company

Configuring Access to the Email Security Appliance

AsyncOS provides administrators controls to manage users' access to the Email Security appliance,

```
        aes256-ctr
        arcfour256
        arcfour128
        aes128-cbc
        3des-cbc
        blowfish-cbc
        cast128-cbc
        aes192-cbc
        aes256-cbc
        arcfour
        rijndael-cbc@lysator.liu.se
MAC Methods:
        hmac-md5
        hmac-sha1
        umac-64@openssh.com
        hmac-ripemd160
        hmac-ripemd160@openssh.com
        hmac-sha1-96
        hmac-md5-96
Minimum Server Key Size:
        1024
KEX Algorithms:
        diffie-hellman-group-exchange-sha256
        diffie-hellman-group-exchange-sha1
        diffie-hellman-group14-sha1
        diffie-hellman-group1-sha1

Choose the operation you want to perform:
- SETUP - Setup SSH server configuration settings
[]> setup

Enter the Public Key Authentication Algorithms do you want to use
```

For *hosting* AsyncOS update files, you must have a server in your internal network that has:

- A web server — for example, Microsoft IIS (Internet Information Services) or the Apache open source server — which:
  - supports the display of directory or filenames in exet 1 Tf8r(s)-9.96 0 0 9.7d29.96 04 innrect

Before You Begin

Determine whether the appliance will download upgrades and updates directly from Cisco, or whether you will host these images from a local server on your network instead. Then set up your network to support the method you choose. See all topics under Setting Up to Obtain Upgrades and Updates, page 33-14.

Procedure

Step 1 Choose **Security Services > Service Updates.**

Step 2 Click **Edit Update Settings**.

Step 3 Enter options:

Setting	Description
Update Servers (images)	Choose whether to download Cisco Iro

Note You cannot load a configuration file with masked passwords using the Configuration File page in the GUI or the `loadconfig` command in the CLI.

c.

PERIODIC_REPORTS. REPORT_TASK.ARCHIVE_FAILURE	A failure occurred while archiving periodic report '$report_title'. This subscription has been removed from the scheduler. Critical. Sent when a report could not be archived.	'**report_title**' - the report title
SENDERBASE.ERROR	Error processing response to query $query: response was $response	'**query**' - The query address. '**response**' - Raw data of respons(s)3.2s(s)( )]TJ-.ScJ-.S30.4(s)

AsyncOS supports “splitting” DNS servers when not using the Internet’s DNS servers. If you are using your own internal server, you can also specify exception domains and associated DNS servers.

When setting up “split DNS,” you should set up the in-addr.arpa (PTR) entries as well. So, for example, if you want to redirect “.eng” queries to the nameserver 1.2.3.4 and all the .eng entries are in the 172.16 network, then you should specify “eng,16.172.in-addr.arpa” as the domains in the split DNS

Editing Time Settings

Reading the Rates of Delivered and Bounced Messages

All rates are shown as the average rate an event occurs per hour at the specific point in time the query is made. Rates are calculated for three in

Example

```
mail3.example.com> rate


Enter the number of seconds between displays.

[10]> 1


Hit Ctrl-C to return to the main prompt.


[10]>
```

The `hostrate` command returns real-time monitoring information about a specific mail host. This information is a subset of the status detail command. (See Monitoring Detailed Email Status, page 34-8.)

Hard Bounced Recipients Delta Difference in the total number of hard bounced recipients to the

Use Control-C to stop the `hostrate` command.

Example

Example

The Cisco appliance gives you various options to delete recipients depending upon the need. The following example show deleting recipients by recipient host, deleting by Envelope From Address, and deleting all recipients in the queue.

Delete by Recipient Domain

- If you use only SNMPv1 or SNMPv2, you must set a community string. The community string does not default to `public`.
- For SNMPv1 and SNMPv2, you must specify a network from which SNMP GET requests are accepted.

```
>

Which port shall the SNMP daemon listen on?

[161]>


Service SNMP V1/V2c requests? [N]> y


Enter the SNMP V1/V2c community string.

[]> public


From which network shall SNMP V1/V2c requests be allowed?

[192.168.2.0/24]>


Enter the Trap target (IP address recommended). Enter "None" to disable traps.

[None]> 10.1.1.29


Enter the Trap Community string.

[]> tcomm


Enterprise Trap Status

1. RAIDStatusChange             Enabled

2s nrindca7.5(c)lur            En    Enabled
```

Frequently Asked Questions

CHAPTER

Network Interface Card Pairing/Teaming

Virtual Local Area Networks (VLANs)

Creating an IP Interface on a VLAN via the interfaceconfig Command

In this example, a new IP interface is created on the VLAN 31 ethernet interface.

```
Currently configured loopback interface:

1. Loopback


Choose the operation you want to performterface:  13[(Choos/T217.5(e omail3.ex.5188 mple.com> 98 0 0R
```

Creating an IP Interface on Loopback via the interfaceconfig Command

Create an IP interface on the loopback interface:

CHAPTER

Spam Quarantine GUI Logs Spam Quarantine logs record actions associated with th

An interesting point to note about ‘rewritten’ entries is that they can appear after lines in the log indicating use of the new MID.

Messages Sent to the Spam Quarantine

When you send a message to the quarantine, the mail logs track the movement to and from the quarantine using the MID (Message ID) and Destination Connection ID

Examples of Bounce Log Entries

Soft-Bounced Recipient (Bounce Type = Delayed)

Hard-Bounced Recipient (Bounce Type = Bounced)

Bounce Log with Message Body and Logheaders

Table 38-12 Status Log Statistics

Domain Debug Log Example

Using Injection Debug Logs

Injection debug logs record the SMTP conversation between the Email Security appliance and a specified host connecting to the system. Injection debug logs are useful for troubleshooting communication problems between the Email Security appliance and a client initiating a connection from

Using Safelist/Blocklist Logs

Table 38-27 shows the statistics recorded in safelist/blocklist logs.

Safelist/Blocklist Log Example

Note

Figure 39-1 Cluster Level Hierarchy

Within each level there will be one or more specific members for which settings may be configured; these are referred to as *modes*. A mode refers to a named member at a specified level. For example, the group "usa" represents one of two group modes in the diagram. While levels are a general term, modes are

Adding Groups

All clusters must contain at least one group. When you create a new cluster, a default group called

Restricted commands, on the other hand, are commands that only apply to a specific mode. For example, users cannot be configured for specific machines — there must be only one user set across the whole cluster. (Otherwise, it would be impossible to login to remote machines with the same login.) Likewise, since the Mail Flow Monitor data, System Overview counters, and log files are only maintained on a

machine only-settings like IP address). The `clusterconfig` command cannot be used to join a remote

The Trace page (and `trace` CLI command) prompts you for the input parameters listed in Table 40-1

Running a Packet Capture

- Name-value pairs for the variable substitution

Part Assembly

Where SMTP uses a single DATA command for each message body, IPMM uses one or many XPRT commands to comprise a message. Parts are assembled based upon the order specified per-recipient.

CHAPTER

Messages that are released from the external quarantine on the Security Management appliance are

Before You Begin

- Review the information in Mail Flow and the External Spam Quarantine, page 42-2.
- Review and take action on the information in Migrating from a Local Spam Quarantine to an

APPENDIX B

IP Addresses, Interfaces, and Routing

When selecting an interface on which to perform a command or function in the GUI or CLI that allows you to select an interface (for example, upgrading AsyncOS, or configuring DNS, etc.), routing (your default gateway) will take precedence over your selection.

For example, suppose you have an Cisco appliance with the 3 network interfaces configured, each on

APPENDIX C

Filtering Messages Based on Content

In this part of the example, you will create three new content filters to be used in the Incoming Mail Policy table. All of these content filters will be editable by delegated administrators belonging to the Policy Administration custom user role. You will create the following:

1. "scan_for_confidential"

   This filter will scan messages for the string "confidential." If the string is found, a copy of the message will be sent to email alias `hr@example.com`, and the message will be sent to the Policy quarantine area.

2.

"Virtual Machine" means a softwa

Content Matching Classifier The detection component of the RSA data loss prevention scanning engine. A classifier contains a number of rules for detecting sensitive data, along with context rules that search fo

I

IDE File — Virus Definition File. An IDE file contains signatures or definitions used by anti-virus software to detect viruses.

L

LDAP — Lightweight Directory Access Protocol. A protocol used to access information about people (including email addresses), organizations, and other resources in an Internet directory or intranet directory.

Listener — A listener describes an email processing service that will be configured on a particular IP interface. Listeners only apply to email entering the Cisco appliance — either from the internal systems within your network or from the Internet. IronPort AsyncOS uses listeners to specify criteria that messages must meet in order to be accepted and relayed to recipient hosts. You can think of a listener as an “email injector” or even a “SMTP daemon” running for each IP address you specify.

IronPort AsyncOS differentiates between *public* listeners — which by default have the characteristics for receiving email from the Internet — and *private* listeners that are intended to accept email only from internal (groupware,

Spam

Unwanted, Unsolicited Commercial bulk Email (UCE/UBE). Anti-spam scanning identifies email messages that are suspected to be spam, according to its filtering rules.

STARTTLS