



IPSWITCH

IMail Server™

IMail Secure Server
as a Mail Gateway

CHAPTER 1 IMail Secure Server as a Mail Gateway

What is a Mail Gateway?.....	1
Mail Gateway Setup	2

CHAPTER 2 Possible Mail Gateway Configurations

Peering.....	3
Domain Forwarding.....	4
External Address Verification.....	4

CHAPTER 3 Filtering Options

Anti-virus Protection.....	6
IMail Anti-virus powered by Commtouch®	6
Commtouch® Zero Hour.....	7
Anti-spam Protection	8
Commtouch® Premium Anti-spam	8
Commtouch IP Reputation (Premium Connection Checks)	8
SPF Filtering.....	8
Domainkeys / DKIM	9
Attachment Blocking	9
Content Filtering	9
Connection Filtering	10

CHAPTER 4 Setting Up an External Address Verifier

Verifier Setup.....	12
MX Record changes for DNS.....	13

CHAPTER 5 Verifier Examples

External Address Verification - Verifier Example	15
External Address Verification - Wildcard Examples	17

CHAPTER 6 For More Assistance

Ipswitch Support.....	18
-----------------------	----

CHAPTER 1

IMail Secure Server as a Mail Gateway

In This Chapter

What is a Mail Gateway?.....1

Mail Gateway Setup.....2

This document was designed as a solutions guide for customers to gain a better understanding of mail gateways; and to provide reasons why mail gateways may be necessary. This document will also explore various options for using IMail Secure Server as a mail gateway.

Although other means of communication are growing in popularity and threatening to replace e-mail; e-mail is still a vital communication tool for the foreseeable future. The greatest challenge e-mail faces today is the massive volume of unwanted junk mail, commonly known as spam. Spam is a huge problem, with recent statistics showing spam taking up as much as 80% of all e-mail traffic. This creates a massive increase in wasted resources; such as higher network bandwidth requirements and employee time. In addition, there are other related e-mail borne security risks such as "phishing" and "malware" that are extremely hazardous to the security of an organization's network. Using a mail gateway can help shield your internal mail server from this hostile environment and help control many of these potential risks.

What is a Mail Gateway?

A mail gateway is a server that is set up in front of your organization's primary mail server, and serves as a buffer for the internal mail server against the hazards of the internet.

Using IMail Secure Server can serve numerous possible purposes:

- 1** To process and filter all incoming mail before it is passed on to the internal mail server that delivers the messages. This can include spam and virus filtering, along with other types of filtering as discussed further below.
- 2** To reduce the amount of traffic to your primary mail server
- 3** To enhance security on your network. An e-mail gateway provides a barrier between your internal network and the internet. Set up correctly, a gateway minimizes the access to your internal network should it ever become compromised.

Mail Gateway Setup

To set up IMail Secure Server as a gateway, a number of factors must be considered. The mail gateway must be setup to allow all mail to flow through for filtering before being forwarded to your internal mail server. Although there are several possible configurations to handle mail flow to a mail gateway; this document will cover a typical configuration.

DNS Setup

When initially setting up a mail gateway, consideration must be made for DNS records. "MX" and "A" records must be configured to point all mail to the gateway server.



Note: All "MX" records must point to an "A" record of the mail gateway server.

DMZ Setup

The next consideration is network connectivity. Normally, a mail gateway is placed in a section of the network that is exposed to the internet, also known as a "Demilitarized Zone" or DMZ. Properly configured this will restrict the mail gateway server's access to the rest of the organization's network, allowing just enough access to connect to the internal mail server and deliver messages to local users.

Possible Mail Gateway Configurations

In This Chapter

Peering	3
Domain Forwarding	3
External Address Verification	4

Once your DNS Server and DMZ are configured, the next step is to decide on the best configuration to forward all e-mail to internal users.

Peering

Peering is a feature that can be set up within an IMail Secure Server on a per-domain level. Your mail gateway will need a domain for each internal mail domain with the same named domain name. For multiple internal mail domains, multiple peer domains must be created on the mail gateway server.

Once peering is set up the peered mail gateway server will evaluate all incoming "RCPT TO" commands based on domain validations and user verifications.

- If the domain validation fails the mail gateway will return a "550" on the "RCPT TO" and the session is terminated.
- If the user is not found locally, a "VRFY" or "RCPT TO" command will be used to check the peered mail server. If this check fails the mail gateway will return a "550" on the "RCPT TO" and the session is terminated.

Peering is a valid way to handle a mail gateway, but has the drawback of requiring the mail gateway to be configured to match all internal mail domains. External Address Verification only requires the administrator to set up a verifier on the mail gateway. The verifier will query an internal user store for the validity of the user by using the incoming "RCPT TO" command. Using this method does not require the mirroring of internal mail server domains.

Domain Forwarding

Domain Forwarding is a feature that is configured within an IMail Secure Server as an option at the SMTP Service level. Domain Forwarding will redirect all mail sent to a specific domain to another IP Address. Your mail gateway will only redirect mail that has domain names configured.

Domain Forwarding like Peering has the drawback of requiring the mail gateway to be configured to match all internal mail domains. Any message that does not find a match when Domain Forwarding is configured will fail mail gateway entry and will return a "550" on the "RCPT TO" with the session terminated.

External Address Verification as stated with Peering only requires the administrator to set up a verifier on the mail gateway. Using this method would not require each mail domain be setup with an IP Address within SMTP for forwarding to your internal mail server domains.

External Address Verification

External Address Verification allows your IMail Secure Server to be the mail gateway, determining whether or not mail recipients are valid users for another destination mail server and to reject all other recipients as invalid.

External Address Verification can be enabled by configuring one or more Address Verifiers. Each Address Verifier identifies e-mail addresses as valid or invalid depending on its configuration. When External Address Verification receives an e-mail address to be verified, it will check each configured Address Verifier to determine whether or not the e-mail address is valid or invalid.

External Address Verification Setup

The External Address Verification (EAV) process in IMail is currently designed for use only with an LDAP / Active Directory database. Creating and configuring an LDAP / Active Directory Address Verifier provides a filtering process that will only allow messages intended valid users to be passed on to the internal mail server.

When External Address Verification is active, and a "RCPT TO" or "VRFY" command are received by SMTP, the following occurs:

- 1 Local host is checked.
- 2 The address is then passed to active Address Verifiers to determine the validity of the message recipient.
- 3 A valid message recipient will be sent a 250 and will be allowed to proceed.
- 4 A message without a valid recipient will usually result in a 550 response, unless SMTP is configured for message relaying.

Address Verifier Caching

Depending on the amount of mail being filtered for verification, External Address Verification can become a CPU intensive process. To ease the strain on the CPU, in-memory caching can be activated to reduce the number of queries being made by the active Address Verifiers. All e-mail addresses that receive a positive result by an Address Verifier will be added to the cache; where they will remain for the configured amount of time. When EAV finds an e-mail address already existing in cache, a valid result will immediately be returned. This is done without running any additional checks with the active Address Verifiers. This will also renew the amount of time the e-mail address will remain in the cache.

Configuration options for the in-memory cache can be found on the External Address Verification page under Advanced Settings. Once caching is enabled, it is recommended to leave the default caching settings. Initially, CPU resources will go up until the cache is filled.



Note: Addresses with negative results from EAV are not cached.

Filtering Options

In This Chapter

Anti-virus Protection6

Anti-spam Protection7

Anti-spam and Anti-virus filtering options can be set up to control and limit unwanted and hazardous e-mail to your local mail servers.

Anti-virus Protection

Using IMail Secure Server as your gateway includes both IMail Anti-virus powered by Commtouch® and Commtouch® Zero Hour.

IMail Anti-virus powered by Commtouch®

IMail Anti-virus powered by Commtouch® works within IMail Secure Server and can simultaneously process with either Symantec™ or BitDefender®. This process is capable due to Commtouch® scanning during the SMTP session, allowing message rejection before being accepted.

Commtouch's Command Anti-virus SDK is available for your IMail Secure Server as another option against the constant battle against undesirable e-mail, including spam and viruses. The Command Anti-virus engine blocks malware of all types, including worms, Trojans and spyware. Command Anti-virus has a proven track history for defending against malware for over 20 years.

IMail Anti-virus powered by Commtouch® works with IMail Secure Server:

- Multi-layered, multi-engined platform using heuristics, emulation, and signatures for maximum protection.
- Zero-Hour detection: architecture geared for fast reaction to new threat types.
- Superior detection and low false positives.
- Upon detection of a possible virus, options can be configured within your IMail Secure Server to delete the message, reject the message, or redirect the message to another address.
- Optionally, A message can be sent to the intended recipients informing them a message could not be delivered.

Commtouch® Zero Hour

Commtouch® Zero Hour works within IMail Secure Server on a per-domain basis and can simultaneously process with either Symantec™ or BitDefender®. This process is capable due to Commtouch® scanning during the SMTP session, allowing message rejection before being accepted.

Server-side polymorphic malware has become impossible for traditional AV engines to block, since there are typically thousands of distinct variants, and malware distributors often release hundreds of new variants per hour. Commtouch® Zero-Hour Virus Outbreak Protection provides a complementary shield to conventional AV technology, protecting in the earliest moments of malware outbreaks, as each new variant emerges.

Commtouch Zero Hour works with IMail Secure Server as follows:

- Security experts agree that signature-less protection is an essential complement to traditional AV technologies. By proactively scanning the Internet and identifying massive virus outbreaks as soon as they emerge, Commtouch's Zero-Hour Solution provides just that: proactive virus blocking that is effective and signature-independent.
- **Immediate.** Commtouch provides proactive virus detection to close the early-hour vulnerability gap during which millions of users are infected. Commtouch's proactive virus detection capabilities ensure users' protection hours before signatures are released.
- Robust and inherently immune to emerging foiling attempts, Commtouch's Zero-Hour Virus Outbreak Protection Solutions are based on RPD technology, which has a track record of protecting million of users globally.
- Upon detection of a possible virus, options can be configured within your IMail Secure Server to delete the message, reject the connection, or forward to another mailbox or address.

Anti-spam Protection

Commtouch® Premium Anti-spam

In addition to the standard anti-spam filter included with all IMail Servers, the optional Premium Filter provides fully automated spam protection. The Premium Filter, provided in partnership with Commtouch Advanced Security Daemon (a.k.a. ctasd™) is a plug-and-play e-mail-borne spam outbreak detection daemon that combines your current core messaging network infrastructure with advanced detection and classification capabilities. The daemon adds a layer of e-mail filtering to your mail delivery system in order to provide real-time classification in the first minutes after a new outbreak is launched.

Commtouch IP Reputation (Premium Connection Checks)

Commtouch's GlobalView™ Mail Reputation works within IMail Secure Server as an e-mail authentication standard that uses public/private encryption and DNS to prove the legitimacy and contents of an e-mail message. Commtouch's IP Reputation services are used primarily to weed out spam messages before these messages enter the customer's messaging network, thereby relieving the need for resource-consuming downstream filtering. This is accomplished by applying the most up-to-date IP reputation data to the IP address of the sender, before the SMTP connection is accepted.

Commtouch IP Reputation delivers cost-effective benefits such as the following:

- Reduce IT resources such as server count, CPU load, storage, etc.
- Eliminating multiple security risks
- Reducing the level of false positives
- Minimizing the cost of downstream filtering
- Lowering the overall bandwidth consumption
- Optimizing IT labor required to manage the overall messaging process

SPF Filtering

IMail uses Sender Policy Framework (SPF) to extend the Simple Mail Transfer Protocol (SMTP) and Domain Name System (DNS) so IMail Secure Server does not accept e-mail unless the sending computer is designated as a legitimate e-mail sender. This feature provides administrators increased capability to stop incoming e-mail from forged (spoofed) e-mail addresses.

To accomplish this e-mail security measure, SPF establishes a policy framework and a sender authentication scheme that verifies the identity of e-mail servers domains for incoming messages. SMTP then uses this information to evaluate whether the message is from an e-mail server that is authorized to send e-mail from the message sender. Messages that do not meet the SPF criteria are not accepted as a legitimate e-mail message and are processed according to the SPF settings set by the IMail Administrator.

Domainkeys / DKIM

DomainKeys and **DomainKeys Identified Mail (DKIM)** are e-mail authentication methodologies designed to verify digitally signed e-mail on a per-domain basis. Both methods were designed for protection of e-mail identity and have assisted in the control of "spam" and "phishing". DomainKeys and DKIM use asymmetric key cryptography to sign messages with a private key and use DNS to distribute the public key for signature verification.

- DomainKeys is a domain-level e-mail authentication standard that uses public/private key encryption and DNS to prove the legitimacy and verify the unchanged contents of an e-mail message. This verifies that the domain used in the "from" or "sender" header of a message has not been modified while in transit.
- DKIM is very similar in functionality to DomainKeys, with an enhanced standard that provides more flexibility and security. Although DKIM does not filter or identify spam, widespread use of DKIM can prevent spammers from forging the source address of their messages. If spammers are forced to show a correct source domain, then the other spam filtering techniques will work more effectively.

Attachment Blocking

According to anti-virus statistics, majority of viruses are spread by users opening attachments by e-mail. Use **Attachment Blocking** to control the attachment types to block from incoming and outgoing e-mail messages and actions to take on blocked messages.

Content Filtering

Content Filtering are domain level spam filtering features that are standard to all IMail Servers. These filters scan the contents of incoming messages for common spam characteristics.

- **Statistical Filter.** Examines each word in the body of an e-mail message to determine if the e-mail is spam.
- **Phrase Filter.** Searches for spam phrases within the body of e-mail messages and identifies the messages that are spam.
- **HTML Features Filter.** Searches HTML features in messages that are subject to spam. Sets how many HTML features must be present in an ".htm" file in order for a message to be identified as spam and the spam action to take.
- **URL Domain Blacklist.** Searches for domain names that appear as URL links in messages, and lets you set the action to take on such messages.
- **Broken MIME Headers.** Uses the Broken MIME Header Filter to identify MIME Header characteristics that result in SPAM e-mail.

Connection Filtering

Connection Filtering are domain level spam filtering features that are standard to all IMail Servers. These filters attempt to verify that incoming messages come from a valid mail server.

- **Verify MAIL FROM Address.** Checking the "From" address of the connecting server to be verified for each message to ensure that the user is a valid user on the mail server. If the user or server does not exist, the message is identified as spam and the IMail Administrator has multiple choices to decide the action to be taken for the message. .
- **Perform Reverse DNS Lookup for Connecting Server.** A reverse DNS lookup to determine the domain name against the IP address of the connecting server is performed. An IP address with no PTR record is usually from a spoofed message an indicator of spam. If there is no reverse record for that IP address the IMail Administrator has multiple choices to decide the action to be taken for the message.
- **Verify HELO / EHLO domain.** A test against the domain passed during the HELO/EHLO is used to perform a DNS query to verify that the domain specified has an A record or an MX record. If this test fails, the IMail Administrator has multiple choices to decide the action to be taken for the message.

Setting Up an External Address Verifier

In This Chapter

Verifier Setup..... 11
MX Record changes for DNS..... 13

Enabling External Address Verification

By default **External Address Verification** is disabled. A decision must be made to enable External Address Verifier's for all domains or only specified domains.

In the web administrator or console administrator go to **System > External Address Verification** and use the drop down at the top of the page to make your selection.

- **Disabled.** (Set by Default) External Address Verifiers are disabled.
- **Enabled.** This option will verify all incoming message recipients as defined by the listed Verifiers.
- **Enabled for Specified Domains.** Selecting this option will only verify message recipients for the domain names specified. All other recipients will be rejected as invalid.

Setting for Specified Domains will enable the entry of external domain names.



Note: When using **Specified Domains**, be sure to enter one domain name per line. Entering domain names correctly is important for mail to be forwarded to all users.

Verifier Setup

Adding and Configuring an Address Verifier

Once you have enabled the verification process an **Address Verifier** can be added.

Adding a Verifier

Click the Add button to configure a **new Address Verifier**, or select an existing verifier and click the Edit button. The dialog that appears will enable configuring a new or existing Address Verifier.

- **Auto Detect For Active Directory.** Check this box if your mail server is on an Active Directory domain. Auto Detect will automatically pull information using the current domain and search all the sub-containers.



Note: The settings used for Auto Detect will not fill user interface text boxes.

- **Enabled.** (Set by Default) Enables verifier for use once saved.
- **Verifier Name.** (Required) Enter a name in the text box to identify the Address Verifier. This can be any name that you want, and will be used in log lines to identify the Address Verifier.
- **Host Address.** The fully qualified domain name or IP address of the LDAP server. The IMail Server will attempt to resolve this information automatically if left blank.
- **Port.** The TCP port for your LDAP Server. Port 389 is the default when left blank.
- **DN.** The **Distinguished Name** of the LDAP container on the server to connect to and query. The IMail Server will attempt a rootDSE call for the Default Naming Context to set the DN when left blank.
- **Username / Password.** Credentials used for connecting to your LDAP Server. Normally this would only be used if the mail server is not a member of the domain being used. If left blank the SMTP Service user context is used, which is normally "`NT authority\LocalSystem`".
- **Filter.** This is an advanced option feature and should only be used with a full understanding of LDAP filter strings. Normally this is used only to connect with a custom LDAP Server. For an Active Directory database `sAMAccountName`, `User Principal Name`, `CN`, and `OpenLDAP uid` are used as part of the default search string.
- **Enable Sub-level Search.** Set by Default. This setting will allow LDAP to search the current container and all sub containers indicated by the DN. Leaving this unchecked will limit LDAP to search only the the container indicated by DN.
- **Authentication Type.** This drop down identifies the Authentication Type to be used with the LDAP Verifier.
- **Secure.** For secure authentication, the Address Verifier will authenticate using NTLM or Kerberos depending on the OS is configuration to use Windows NT or an Active Directory provider. This is the value that will be used when the Auto Detect is being used.

- **ServerBind.** Uses standard LDAP authentication against the server. This should be used when connecting to other LDAP servers (including the IMail LDAP Server).



Note: If the Active Directory path includes a server name, then specify this flag when using LDAP. Do not use this flag for paths that include a domain name or for serverless paths.

- **Anonymous.** Selected this setting only if the LDAP does not require authentication.
- **Test Verifier.** Click this button to test the current verifier settings. Saving is not required for use of the test button.
- **Address to Verify.** E-mail address to test.

Click **OK** to add the **External Address Verifier**. The new verifier will appear on the External Address Verification list, but will not be permanent until the "**Save**" button is clicked.



Note: **SMTP** services must be restarted for the new verifier to become active.

MX Record changes for DNS

Once your External Verifiers are tested and working, the final step to activate your mail gateway is to update your MX records in DNS. All MX records that currently exist for your mail domains on your DNS Server must be updated and point to the mail gateway server.

CHAPTER 5

Verifier Examples

In This Chapter

External Address Verification - Verifier Example 14

External Address Verification - Wildcard Examples..... 16

For custom LDAP / Active Directory examples visit the following *Knowledge Base* article: http://kb.imailserver.com/cgi-bin/imail.cfg/php/enduser/std_adp.php?p_faqid=1280

External Address Verification - Verifier Example

Active Directory Verifier

Example

The following verifier is explained below

Configure Address Verifier

LDAP / Active Directory

Verifier Enabled

Name:

Auto Detect for Active Directory

Host Address:

Port:

DN:

Username:

Password:

Filter:

Enable Sublevel Search

Authentication Type:

Test Settings

Address to Verify:

Result:
Address accepted - Address: salesuser1

- **Auto Detect For Active Directory.** "Not checked" as this verifier is not on the specified domain.
- **Enabled.** (Set by Default) Enables verifier for use once saved.
- **Verifier Name.** (Required) "qatest" Name set to identify the LDAP Verifier.
- **Host Address.** "192.168.6.225" The IP address of the Active Directory server.
- **Port.** Left blank defaults to port 389 .

Mail Gateway Solutions

- **DN.** "dc=gatest,dc=local" The domain component that will be connected and queried.
- **Username / Password.** "user1" Credentials to be used to connect.
- **Filter.** No filter in place. The default filter will be used.
- **Enable Sub-level Search.** "Enabled" To search the current container and all sub containers indicated by the DN.
- **Authentication Type.** Secure.
- **Address to Verify.** salesuser1 verified.

External Address Verification - Wildcard Examples

Wildcard Usage for Domain Names

Example 1 (No Wildcards):

External Address Verification is enabled for specified domains. Only the following specified domain names will be available for External Address Verification. No wildcard usage is made.

Domain Name
"mail.domain.com"
"mail.subname.domain.com"
"subname.domain.com"
"domain.com"

Example 2 (Wildcard Usage):

External Address Verification is enabled for specified domains. The following are examples of **valid and invalid wildcards designed for External Address Verification**.

Domain Name	
*.domain.com	<ul style="list-style-type: none"> ▪ mail.domain.com - VALID ▪ mail.dude.domain.com - VALID ▪ subway.atlanta.domain.com - VALID ▪ mail.newyorkdomain.com - NOT VALID ▪ domain.noway.com - NOT VALID
<ul style="list-style-type: none"> ▪ *domain.com 	<ul style="list-style-type: none"> ▪ mail.newyorkdomain.com - VALID ▪ domain.noway.com - VALID ▪ mail.domain.com - NOT VALID ▪ mail.dude.domain.com - NOT VALID ▪ subway.atlanta.domain.com - NOT VALID
<ul style="list-style-type: none"> ▪ domain*.com 	NOT A VALID WILDCARD
dom*.com	NOT A VALID WILDCARD
dom*	NOT A VALID WILDCARD
domain.*	NOT A VALID WILDCARD
.domain.com	NOT A VALID WILDCARD - Only one asterisk is honored and handled as a wildcard.

CHAPTER 6

For More Assistance

In This Chapter

Ipswitch Support 18

Ipswitch Support

The Ipswitch Support Center provides a multitude of product related resources such as Knowledge Base articles, peer support forums, patches and documentation downloads. It also lists Ipswitch's Technical Support staff's contact information, hours of operation, and information about service agreements.

You can access the support center at:

<http://www.imailserver.com/support/>