



WebSense Support Webinar: Questions and Answers

Pre-screening in Websense Email Security Websense Email Security™ Version 6.1

Question: How does Websense Email Security stop IP spoofing?

Answer: IP spoofing is a challenging problem, because it is inherent in the design of the TCP/IP protocol. Typically, IP spoofing is used in Denial of Service (DoS) attacks. Crackers are concerned only with consuming bandwidth and resources; they don't need to worry about properly completing handshakes and transactions. Rather, they wish to flood the victim with as many packets as possible in a short amount of time.

Websense Email Security can deploy the Denial of Service Detection tool, which monitors the number of incomplete SMTP sessions from individual IP addresses per hour. If a threshold figure is exceeded for a specific IP, connections from that sending IP address can be denied.

Question: How do I search the logs for specific email violations?

Answer: You use a tool called Message Search. This is a feature of Message Administrator that is designed to interact with and manage quarantined messages. It allows you to search any of the following details: Sender, Recipient, Date.

After your search is completed, you are able to view the disposition of a message with an additional feature called Message History.

Question: Can you integrate Websense Email Security with an existing Websense Web filtering server?

Answer: Websense Email Security can run in the same network with Websense Web Security Suite, as long as they are installed on different server machines. In this situation, email filtering and Web filtering remain separate processes (not integrated). You can install Websense Email Security on the *same* server as Websense Express. In that situation also, the products work independently.

Question: How does Websense Email Security differ from offerings from Symantec or Cisco?

Answer: Websense Email Security puts you in control. It allows you create and manage the security settings and policies that suit your specific environment.



Question: Some configurations mention Connection Management. Which features are those exactly?

Answer: Connection Management refers to these features:

- Protected Domains
- Mail Relays
- Blacklists
- Reverse DNS Lookup
- Reputation Service/DNS Blacklists
- Directory Harvest Detection
- Remote User Authentication
- Sender Policy Framework Check

Question: What is True Source IP?

Answer: True Source IP is the IP address from which the message originated. The True Source IP Detection feature in Websense Email Security enables its Connection Management features to be fully effective, even when Websense Email Security is installed downstream from a firewall or an internal mail relay. Instead of using the IP of the connecting, upstream Mail Transfer Agent, True Source IP Detection uses the information in the message header to determine the IP address of the first sender (True Source IP) outside the network perimeter.

Question: When Directory Harvest Detection (LDAP) rejects and locks out future connections for one hour, are there thresholds you can set? Or will it lock out the sender after one wrong email address.

Answer: Websense Email Security detects when a server is trying to send a large number of messages for the purpose of directory harvesting, by keeping a count of:

- The number of invalid email addresses or domains per connection
- The number of invalid email addresses or domains from each IP address per hour

You can configure the Receive Service to terminate a connection when these counts reach a pre-set maximum.

Question: How do I view the logs for messages that were blocked using Reverse DNS Lookup?

Answer: A Connection Disposition table is located within the Connection Log. Whenever the Reverse DNS Lookup feature has blocked a connection, the Connection Disposition table displays the Reverse DNS Lookup. In addition, an Event Table provides additional details of the blocked connection.



Question: Does remote user authentication allow authentication against a directory (LDAP)?

Answer: No; remote user authentication must be configured manually.

Question: We are currently migrating from GW to Exchange Server 2007. Our external domain is a **.org**, but our Active Directory domain is a **.local**. We have all of our recipients set up in the **.local**. Should I add the **.local** to the protected domain?

Answer: You should add the domain included in the email address being used. For example, if the email address is bob@mydomain.com, then the protected domain should be mydomain.com. This is the header information that is checked by the Receive Service.