AMENDMENTS TO THE CLAIMS

1. (Amended). A system for detecting and selectively removing viruses in data transfers, the system comprising:

a memory for storing data and routines, the memory having inputs and outputs, the memory including a server for scanning data for a virus and specifying data handling actions dependent on an existence of the virus;

a communications unit for receiving and sending data in response to control signals, the communications unit having an input and an output;

a processing unit for receiving signals from the memory and the communications unit and for sending signals to the memory and communications unit; the processing unit having inputs and outputs; the inputs of the processing unit coupled to the outputs of memory and the output of the communications unit; the outputs of the processing unit coupled to the inputs of memory, the input of the communications unit, the processor controlling and processing data transmitted through the communications unit to detect viruses and selectively transfer data depending on the existence of viruses in the data being transmitted;

a proxy server for receiving data to be transferred, the proxy server scanning the data to be transferred for viruses and controlling transmission of the data to be transferred according to preset [handing] <u>handling</u> instructions and the presence of viruses, the proxy server having a data input a data output and a control output the data input coupled to receive the data to be transferred; and

a daemon for transferring data from the proxy server in response to control signals from the proxy server, the daemon having a control input, a data input and a data output the control input of the daemon coupled to the control output of the proxy server for receiving control signals, and the data input of the daemon coupled to the data output of the proxy server for receiving the data to be transferred.

2. (Original). The system of claim 1, wherein the proxy server is a FTP proxy server that handles evaluation and transfer of data files, and the daemon is an FTP daemon that communicates with a recipient node and transfers data files to the recipient node.

3. (Original). The system of claim 1, wherein the proxy server is a SMTP proxy server that handles evaluation and transfer of messages, and the daemon is an SMTP daemon that communicates with a recipient node and transfers messages to the recipient node.

4. (Original). A computer implemented method for detecting viruses in data transfers between a first computer and a second computer, the method comprising the steps of:

receiving at a server a data transfer request including a destination address;

electronically receiving data at the server;

determining whether the data contains a virus at the server;

performing a preset action on the data using the server if the data contains a virus;

sending the data to the destination address if the data does not contain a virus;

determining whether the data is of a type that is likely to contain a virus; and

transmitting the data from the server to the destination without performing the steps of determining whether the data contains a virus and performing a preset action if the data is not of a type that is likely to contain a virus.

5. (Original). The method of claim 4, further comprising the steps of storing the data in a temporary file at the server after the step of electronically

transmitting; and wherein the step of determining includes scanning the data for a virus using the server.

6. (Original). The method of claim 5, wherein the step of scanning is performed using a signature scanning process.

7. (Original). The method of claim 4, wherein the step of performing a preset action on the data using the server comprises performing one step from the group of:

transmitting the data unchanged;

not transmitting the data; and

storing the data in a file with a new name and notifying a recipient of the data transfer request of the new file name.

8. (Amended). The method of claim 4, wherein the step of determining whether the data is of a type that is likely to contain a virus is performed by comparing an extension type of a file name for the data to a group [or] <u>of</u> known extension types.

9. (Original). The method of claim 4, further comprising the steps of:

determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network; wherein the server is a FTP proxy server;

wherein the step of electronically receiving data comprises the steps of transferring the data from a client node to the FTP proxy server, if the data is not being transferred into the first network; and

wherein the step of electronically receiving data comprises the steps of transferring the data from a server task to an FTP daemon, and then from the FTP daemon to the FTP proxy server if the data is being transferred into the first network.

10. (Original). The method of claim 4, further comprising the steps of:

determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network;

wherein the server is a FTP proxy server;

wherein the step of sending the data to the destination address comprises transferring the data from the FTP proxy server to a node having the destination address, if the data is being transferred into the first network; and

wherein the step of sending the data to the destination address comprises transferring the data from the FTP proxy server to a FTP daemon, and then from an FTP daemon to a node having the destination address, if the data is not being transferred into the first network.

11. (Currently Amended) A computer implemented method for detecting viruses in a mail message transferred between a first computer and a second computer, the method comprising the steps of:

receiving a mail message request including a destination address;

electronically receiving the mail message at a server;

determining whether the mail message contains a virus, the determination of whether the mail message contains a virus comprising determining whether the mail message includes any encoded portions, storing each encoded portion of the mail message in a separate temporary file, decoding the encoded portions of the mail message to produced decoded portions of the mail message, scanning each of the decoded portions for a virus, and testing whether the scanning step found any viruses;

performing a preset action on the mail message if the mail message contains a virus; and

sending the mail message to the destination address if the mail message does not [contains] contain a virus.

12. (Original). The method of claim 11, wherein the step of determining whether the mail message includes any encoded portions searches for uuencoded portions.

13. (Currently Amended) A computer implemented method for detecting viruses in a mail message transferred between a first computer and a second computer, the method comprising the steps of:

receiving a mail message request including a destination address;

electronically receiving the mail message at a server; scanning the mail message for encoded portions; determining whether the mail message contains a virus;

performing a preset action on the mail message if the mail message contains a virus;

sending the mail message to the destination address if the mail message does not [contains] <u>contain</u> a virus; and

wherein the step of sending the mail message to the destination address is performed if the mail message does not contain any encoded portions; the server includes a SMTP proxy server and a SMTP daemon; and the step of sending the mail message comprises transferring the mail message from the SMTP proxy server to the SMTP daemon and transferring the mail message from the SMTP daemon to a node having an address matching the destination address.

14. (Original). The method of claim 11, wherein the step of determining whether the mail message contains a virus, further comprises the steps of:

storing the message in a temporary file;

scanning the temporary file for viruses; and

testing whether the scanning step found a virus.

15. (Original). The method of claim 11, wherein step of scanning is performed using a signature scanning process.

16. (Original). The method of claim 11, wherein the step of performing a preset action on the mail message comprises performing one step from the group of:

transferring the mail message unchanged;

not transferring the mail message;

storing the mail message as a file with a new name and notifying a recipient of the mail message request of the new file name; and

creating a modified mail message by writing the output of the determining step into the modified mail message and transferring the mail message to the destination address.

17. (Currently Amended). The method of claim 11, wherein the step of performing a preset action on the mail message comprises performing one step from the group of:

transferring the mail message unchanged;

transferring the mail message with the encoded portions having a virus deleted; and

renaming the [encode] <u>encoded</u> portions of the mail message containing a virus, and storing the renamed portions as files in a specified directory on the server and notifying a recipient of the renamed files and directory; and

writing the output of the determining step into the mail message in place of respective encoded portions that contain a virus to create a modified mail message and sending the modified mail message.

18. (Original). An apparatus for detecting viruses in data transfers between a first computer and a second computer, the apparatus comprising:

means for receiving a data transfer request including a destination address;

means for electronically receiving data at a server;

means for determining whether the data contains a virus at the server;

means for performing a preset action on the data using the server if the data contains a virus; and

means for sending the data to the destination address if the data does not contain a virus.

19. (Original). The apparatus of claim 18, wherein means for determining includes a means for scanning that scans the data using a signature scanning process.

20. (Original). The apparatus of claim 18, wherein the means for performing a preset action comprises:

means for transmitting the data unchanged;

means for not transmitting the data; and

means for storing the data in a file with a new name and notifying a recipient of the data transfer request of the new file name.

21. (Original). The apparatus of claim 18; further comprising:

a second means for determining whether the data is of a type that is likely to contain a virus; and

means for transmitting the data from the server to the destination without performing the steps of scanning, determining, performing and sending, if the data is not of a type that is likely to contain a virus.

22. (Original). The apparatus of claim 18, further comprising means for determining whether the data is being transferred into a first network by comparing the destination address to valid addresses for the first network

23. (New). A computer implemented method for detecting viruses in a mail message transferred between a first computer and a second computer, comprising:

receiving a mail message request including a destination address;

electronically receiving the mail message at a server;

determining whether the mail message contains a virus, the determination of whether the mail message contains a virus comprising (i) determining whether the mail message includes any encoded portions, (ii) storing each encoded portion of the mail message in a separate temporary file, (iii) decoding the encoded portions of the mail message to produce decoded portions of the mail message, (iv) scanning each of the decoded portions for a virus, (v) scanning each unencoded portion of the mail message for a virus, (vi) determining if any of the decoded portions of the mail message contain a virus; and (vii) determining if the unencoded portions of the mail message contain a virus;

performing a preset action on the mail message if any of the decoded portions of the mail message contain a virus or if the unencoded portions of the mail message contain a virus; and

sending the mail message to the destination address if the mail message does not contain a virus.

24. (New). A computer implemented method for detecting viruses in a mail message transferred between a first computer and a second computer, comprising:

receiving a mail message request including a destination address;

electronically receiving the mail message at a server;

determining whether the mail message includes any encoded portions;

storing each encoded portion of the mail message in a separate temporary file;

decoding the encoded portions of the mail message to produce decoded portions of the mail message;

scanning each of the decoded portions for a virus;

testing whether the scanning step found any viruses; and

performing one of i) a preset action on the mail message if the mail message contains a virus; ii) sending the mail message to the destination address without first scanning the mail message for viruses if the mail message does not contain any encoded portions; and iii) sending the mail message to the destination address if the encoded portions of the mail message do not contain a virus.

25. (New). The method of claim 24, wherein performing a preset action on the mail message comprises creating a modified mail message without any viruses and transferring the mail message to the destination address.

26. (New). The method of claim 24, wherein the performing a preset action on the mail message comprises transferring the mail message with the encoded portions having a virus deleted.

27. (New). A computer implemented method for detecting viruses in all mail messages transferred between a first computer and a second computer, comprising:

receiving a mail message request including a destination address;

electronically receiving the mail message at a server;

determining for all messages received at the server whether the mail message contains a virus, the determination of whether the mail message contains a virus comprising (i) determining whether the mail message includes any encoded portions, (ii) storing each encoded portion of the mail message in a separate temporary file, (iii) decoding the encoded portions of the mail message to produce decoded portions of the mail message, (iv) scanning each of the decoded portions for a virus, (v) scanning each unencoded portion of the mail message for a virus, (vi) determining if any of the decoded portions of the mail message contain a virus; and (vii) determining if the unencoded portions of the mail message contain a virus;

performing a preset action on the mail message if any of the decoded portions of the mail message contain a virus or if the unencoded portions of the mail message contain a virus; and

sending the mail message to the destination address if the mail message does not contain a virus.

28. (New). A computer implemented method for detecting viruses in all mail messages transferred between a first computer and a second computer, comprising:

receiving a mail message request including a destination address;

electronically receiving the mail message at a server;

determining for all mail messages received at the server whether the mail message includes any encoded portions;

storing each encoded portion of the mail message in a separate temporary file;

decoding the encoded portions of the mail message to produce decoded portions of the mail message;

scanning each of the decoded portions for a virus;

testing whether the scanning step found any viruses; and

performing at least one of i) a preset action on the mail message if the mail message contains a virus; ii) sending the mail message to the destination address without first scanning the mail message for viruses if the mail message does not contain any encoded portions; and iii) sending the mail message to the destination address if the encoded portions of the mail message do not contain a virus.

29. (New). The method of claim 28, wherein performing a preset action on the mail message comprises creating a modified mail message without any viruses and transferring the mail message to the destination address.

30. (New). The method of claim 28, wherein the performing a preset action on the mail message comprises transferring the mail message with the encoded portions having a virus deleted.

31. (New). A computer implemented method for detecting viruses in a mail message transferred between a first computer and a second computer, comprising:

receiving a mail message request including a destination address;

electronically receiving the mail message at a server, wherein the server includes a Simple Mail Transfer Protocol (SMTP) proxy server and a SMTP daemon;

determining if the mail message has encoded portions;

scanning, subsequent to the determining, the encoded portions of the mail message for a virus;

performing at least one of i) a preset action on the mail message if one or more of the encoded portions of the mail message contains a virus; ii) sending the mail message to the destination address without carrying out the determining step if the mail message does not contain an encoded portion; and iii) sending the mail message to the destination address if the encoded portion of the mail message does not contain a virus; and

wherein sending the mail message comprises transferring the mail message from the SMTP proxy server to the SMTP daemon and transferring the mail message from the SMTP daemon to a node having an address matching the destination address.

32. (New). The method of claim 31, wherein performing a preset action on the mail message comprises creating a modified mail message without any viruses and transferring the mail message to the destination address.

33. (New). The method of claim 31, wherein the performing a preset action on the mail message comprises transferring the mail message with the encoded portions having a virus deleted.

34. (New). A computer implemented method for detecting viruses in all mail messages transferred between a first computer and a second computer, comprising:

receiving a mail message request including a destination address;

electronically receiving the mail message at a server, wherein the server includes a Simple Mail Transfer Protocol (SMTP) proxy server and a SMTP daemon;

determining if the mail message has an encoded portion;

scanning each mail message for a virus;

performing a preset action on the mail message if the mail message contains a virus; and

sending the mail message to the destination address if either the mail message does not contain a virus or the mail message does not contain any encoded portions, wherein the sending comprises transferring the mail message from the SMTP proxy server to the SMTP daemon and transferring the mail message from the SMTP daemon to a node having an address matching the destination address.

35. (New). A computer implemented method for detecting viruses in data transfers between a first computer, a server comprising a proxy server, and a second computer, the computer implemented method comprising:

transmitting, by the first computer, a data transfer request including a destination address of the second computer;

receiving at the server the data transfer request and the destination address;

electronically receiving data at the server in response to the data transfer request;

determining, by the proxy server, whether the data contains a virus, wherein the server utilizes a protocol layer hierarchy that includes an application layer, and wherein the proxy server resides below the application layer and detection of a virus by the proxy server occurs below the application layer;

performing, by the server, a preset action on the data if the data contains a virus;

sending the data to the destination address of the second computer if the data does not contain a virus;

determining, by the proxy server, whether the data is of a type that is likely to contain a virus; and

transmitting the data, in response to the data transfer request, from the server to the destination of the second computer without determining whether the data contains a virus and without performing a preset action if the data is not of a type that is likely to contain a virus.

36. (New). A computer implemented method for detecting viruses, comprising:

receiving, at a server comprising a proxy server, a data transfer request, data, and a destination address;

determining, by the proxy server, whether the data contains a virus, wherein the server utilizes a protocol layer hierarchy that includes an application layer, and wherein the proxy server and detection of a virus by the proxy server occurs below the application layer;

performing, by the server, a preset action on the data if the data contains a virus;

sending the data to the destination address if the data does not contain a virus;

determining, by the proxy server, whether the data is of a type that is likely to contain a virus; and

transmitting the data from the server to the destination address without determining whether the data contains a virus and without performing a preset action if the data is not of a type that is likely to contain a virus.

37. (New). The method of claim 11, wherein the step of performing a preset action on the mail message comprises creating a modified mail message by writing the output of the determining step into the modified mail message and transferring the mail message to the destination address.