

DATA DIODE NETWORK AND METHOD THEREFORE

Field of the Invention

[0001] The present invention relates to data diode. Specifically, the present
5 invention relates to a system and method for implementing data diode network.

Background

[0002] Most, if not all, telecommunications and applications are implemented on
10 Hypertext Transfer Protocol (HTTP) framework. It is an application-level protocol
adapted for distributed and collaborative information system over a Transmission
Control Protocol (TCP) connection. It functions as a request-response protocol in the
client-server computing model. In such client-server computing model, a server is
adapted for hosting a website running an application, whilst the client maybe a web
15 browser or web application adapted for accessing the website. Operationally, the client
submits an HTTP request message to the server and the server returns a response message
to the client. The response contains completion status information about the request and
may also contain requested content (aka payload) in its message body. The request-
response between the client and the server are known as HTTP session.

20

[0003] Data diodes are adapted to partition a trusted network from an untrusted
one. Such separation is known as network segmentation/separation. To protect a source
network, the data diode can be deployed at the edge of a security border of the source
network, whereby it allows only outgoing dataflow and prevents all incoming dataflow.
25 Such network is secured from external cyber threat.

[0004] Another use of the data diodes is adapted to protect data designation
network, for example, from data leakage. The data diodes in this case is adapted in a
reverse configuration whereby the network allows only incoming dataflow but prevents
30 all outgoing dataflow. Such network is secure from data leakage.

[0005] It is well understood that as data is encrypted from end to end, it requires that the transmission between the sender and the indented recipient be bidirectional to carry out the handshaking for successful encryptions and decryptions between parties. Such protocol is not implementable over a unidirectional network.

5

Summary

[0006] In one aspect of the present invention, there is provided a data diode module for establishing a request-response connection between a client and a server as two connecting ends over a communication network. The data diode module comprises two independent connection paths, each having a data diode connected on each connection path forming a unidirectional transmission channel within the data diode module, the two data diodes are disposed in an opposing data direction; and two data diode gateways, each connected at a terminating end of the two independent connection paths, wherein the data diode gateways are adapted for mapping and managing connection end points in a manner that each of the data diode gateways serves as an IP Endpoint to the respective connecting end to establish the request-response connection between the connecting end and the data diode gateway, the data diode gateway on one side further conveys messages from the connecting end to the data diode gateway on another side.

20

[0007] In one embodiment, each independent connection path further comprises a checker for detecting and controlling network traffic based on predetermined rules. The checker may further comprise a whitelist.

25

[0008] In a further embodiment, the checker is disposed before the data diode on each independent connection path. Further, a second data diode disposed before the checker on each independent connection path may further be included.

[0009] In yet a further embodiment, the data diode module operationally receives a request from the connecting end, the data diode gateway receives and conveys the request to the another data diode gateway through one of the independent connection paths, whereby the another data diode gateway sends a corresponding request to the receiving connecting end, and upon receiving the corresponding request at the receiving

30

connecting end, the receiving connecting end sends a response to the another data diode gateway, thereby establish a request-response connection between the another data diode gateway and the receiving connecting end. The another data diode gateway receives the response from the receiving connecting end and conveys the response to the data diode gateway through another one of the independent connection paths, the data diode gateway sends a corresponding response to the connecting end with the corresponding response, thereby establishing a request-response connection between the data diode gateway and the connecting end.

10 **[0010]** In another aspect of the present invention, there is also a provided a data diode network adapting the aforesaid a data diode module.

15 **[0011]** In a further aspect, there is provided a method for establishing request-response connections over a data diode network having a client and a server at two connecting ends. The method comprises deploying a data diode module on the data diode network having two independent connection paths, each having a data diode connected on one independent connection path forming a unidirectional transmission channel within the data diode module, wherein the two data diode are disposed in an opposing data direction, the data diode module further comprises two data diode gateways, each
20 connected at a terminating end of the two independent connection paths; receiving, by a data diode gateway of the data diode module connected at one terminating end of the two independent connection paths, a request from one connecting end; conveying the request to another data diode gateway of the data diode module connected at another terminating end of the two independent connection paths; sending a corresponding request to the
25 receiving connecting end; responding, by the receiving connecting end, to the another data diode gateway with a response to establish a request-response connection between the another data diode gateway and the receiving connecting end; conveying the respond to the data diode gateway through another one of the independent connection paths; and sending a corresponding response to the connecting to establish a request-response
30 connection between the data diode gateway and the connecting end.

[0012] In another embodiment, the aforesaid data diode module is deployed.

Brief Description of the Drawings

[0013] This invention will be described by way of non-limiting embodiments of the present invention, with reference to the accompanying drawings, in which:

5

[0014] FIG. 1 illustrates a schematic block diagram of a data diode network in accordance with an embodiment of the present invention;

[0015] FIG. 2 illustrates a schematic block diagram of a data diode network in accordance with another embodiment of the present invention;

10

[0016] FIG. 3 illustrates a schematic block diagram of a data diode network in accordance with a further embodiment of the present invention;

[0017] FIG. 4 illustrates a schematic block diagram of a data diode network in accordance with yet a further embodiment of the present invention; and

15

[0018] FIG. 5 illustrate a flow chart of establishing request-response connections through a data diode network in accordance with one embodiment of the present invention.

20

Detailed Description

[0019] In line with the above summary, the following description of a number of specific and alternative embodiments are provided to understand the inventive features of the present invention. It shall be apparent to one skilled in the art, however that this invention may be practiced without such specific details. Some of the details may not be described at length so as not to obscure the invention. For ease of reference, common reference numerals will be used throughout the figures when referring to the same or similar features common to the figures.

25

30

[0020] FIG. 1 illustrates a schematic block diagram of a data diode network in accordance with an embodiment of the present invention. More suitably, the embodiments of the present invention are applicable over a HTTP network. For purpose

of illustrations herein below, HTTP protocol is adopted in this description. It is understood to a skilled person that the present invention is applicable for any 2-ways data exchange over TCP/IP connections or transmissions. The data diode network **100** concerns communications between a HTTP client **110** and a HTTP server **120**. The

5 HTTP client **110** can be a web browser, such as Google Chrome, Microsoft's Edge, Safari, Firefox or any web applications, such as web service application.

[0021] During a HTTP session, between two IPEndpoints, the HTTP client **110** is required to put a request to the HTTP server **120**, whereby the HTTP server **120**

10 processes the request and return with a response. Accordingly, between the two IPEndpoints, there requires a bidirectional or bilateral request-respond be carried out at a same connection (i.e. a same pair of IPEndpoint) between the HTTP server **120** and the HTTP client **110**.

15 [0022] In normal circumstances, when one data diode is implemented on the communication channel, in either direction of dataflow, the request-respond session cannot be established, as request-respond session requires bidirectional or bilateral communications. Accordingly, a data diode module of embodiments of the present invention is implemented to enable the HTTP sessions between the HTTP client **110** and

20 the HTTP server **120** (i.e. establishing TCP connection, HTTP client sends request, the HTTP server process request and respond to the HTTP client) be carried out.

[0023] In the present embodiment, the data diode module **150** comprises a data diode added on both incoming and outgoing transmissions respectively, i.e. an incoming

25 data diode **150a** and an outgoing data diode **150b** are added. The data diode module **150** further comprises data diode gateways **130a** and **130b** disposed at the two terminating ends of the data diode module **150** respectively. With the data diode module **150** in accordance with the present embodiment added, HTTP sessions can be carried out seamlessly.

30

[0024] The data diode gateways **130a** and **130b** are disposed at the two terminating ends of the data diodes **150a** and **150b**. The data diode gateway **130a** simulate/emulate the intended receiving end to establish the HTTP session. The data

diode gateway **130b** simulates/emulates the receiving end to establish the HTTP session with HTTP server **120**.

[0025] Taking the communication between the HTTP client **110** and the HTTP
 5 server **120** for example, the HTTP client **110** sends a request to the HTTP server **120**.
 As the request reaches the data diode gateway **130a**, the data diode gateway **130a** relays
 the request to the data diode gateway **130b** through the data diode **150a**. Then the data
 diode gateway **130b** acts as an IPEndpoint to the HTTP server **120** and sends a request
 thereto. As the HTTP server **120** receives the request, it processes the same and returns
 10 with a response to data diode gateway **130b**. When the data diode gateway **130b** receives
 the response, the gateway relays the response to the data diode gateway **130a** through
 the data diode **150b**. The data diode gateway **130a** maps the response to a corresponding
 IPEndpoint of the HTTP client **110** and then send the response to the HTTP client **110**.
 It is to be noted that the data diode module **150** allow also payloads to be transmitted
 15 across the data diode module **150** in both directions.

[0026] FIG. 2 illustrates a schematic block diagram of data diode network **200** in
 accordance with another embodiment of the present invention. The data diode network
200 is generally in a same configuration as the data diode network **100** except that the
 20 data diode network **200** comprise a data diode module **250**. The data diode module **250**
 includes an inbound checker **255**, an inbound data diode **250a** and an outbound data
 diode **250b**. For the purpose of this application, as the invention is adapted to mainly
 protect the HTTP server **120**, the terms inbound and outbound are used with reference to
 the data flow into the HTTP server **120**. The inbound checker **255** is disposed prior to
 25 the inbound data diode **250a** whereby the data flows into the HTTP server **120** is being
 processed before entering. In the current embodiment, the inbound checker **255** is
 disposed before the inbound diode **250a** in relation to the data flow direction whereby
 the unnecessary transmission is checked and filtered before entering the inbound data
 diode **250a**. The data diode module **250** further comprises data diode gateways **230a** and
 30 **230b** disposed at the two terminating ends of the data diode module **250** respectively.

[0027] The data diode gateways **230a** and **230b** are disposed at the two
 terminating ends of the data diodes **250a** and **250b**, which are adapted to interface with

the originate sending end. In one embodiment, the data diode gateway is acting as a receiving IPEndpoint for the sending end and the data diode gateway **230a** simulates/emulates the HTTP server for HTTP client to establish HTTP session. For example, when the HTTP client is the sending end, which form an IPEndpoint at the sending end to connect to IPEndpoint at data diode gateway **230** to establish the HTTP session. The data diode gateway **230b** simulate/emulates a HTTP client to communicate with HTTP server **120**.

[0028] The request-respond transmissions between the HTTP client **110** and the HTTP server **120** shall be similar to that in FIG. 1.

[0029] In one embodiment, the inbound checker **255** is a whitelist checker.

[0030] In one embodiment, the inbound checker **255** is adapted to check for malware or any malicious embedded codes. Example of checker means can be true file type detector, static code analyser, multi-antivirus detector, machine learning antivirus or the like, input validation checker, for cleansing the data.

[0031] FIG. 3 illustrates a schematic block diagram of data diode network **300** in accordance with a further embodiment of the present invention. The data diode network **300** is generally in the same configuration as the data diode network **100** except that the data diode network **300** comprises a data diode module **350**. The data diode **350** comprises an inbound checker **352**, an inbound data diode **350a**, an outbound checker **354** and an outbound data diode **350b**. The inbound checker **352** is disposed prior to the inbound data diode **350a** whereby the data flows into the HTTP server **120** is being verified before entering the data diode. The inbound checker **352** is adapted to ensure that the HTTP server **120** is free of malware or the like. The outbound checker **354** is disposed prior to the outbound diode **350b**, whereby data flows out from the HTTP server **120** is being processed and filtered after leaving the HTTP server **120**. The purpose of the outbound checker **354** is adapted for preventing data leaks.

[0032] The outbound checker **354** operationally can be any data loss prevention software that identifies if any of the unintended data flow leaving the HTTP server **120**.

It ensures that the traffic leaving the HTTP server **120** only contains the required information.

[0033] Similarly, the data diode module **350** further comprises data diode
5 gateways **330a** and **330b** disposed at the two terminating end of the data diode module **350** respectively.

[0034] The data diode gateways **330a** and **330b** are disposed at the two
terminating ends of the data diodes and checkers, which are adapted to interface and
10 manage HTTP connections and sessions with the HTTP client **110** and the HTTP server **120** acting as a simulated/emulated HTTP server and HTTP client to the HTTP client **110** and the HTTP server **120** for enabling request-response session as provided above.

[0035] FIG. 4 illustrates a schematic block diagram of data diode network **400** in
15 accordance with yet a further embodiment of the present invention. The data diode network **400** is generally in the same configuration as the data diode network **100** except that the data diode network **400** comprises a data diode module **450**. The data diode module **450** comprises an inbound checker **452**, two inbound data diodes **450a**, **450b**, an outbound checker **454** and two outbound data diodes **450c**, **450d**. The inbound checker
20 **452** is disposed between to the two inbound data diode **450a**, **450b** whereby the data flows into the HTTP server **120** is being verified before entering. The inbound checker **452** is adapted to ensure that the HTTP server **120** is free of malware. The outbound checker **454** is disposed between the two outbound diode **450c**, **450d** whereby data flows out from the HTTP server **120** is being processed and filtered after leaving the HTTP
25 server **120**. The purpose of the outbound checker **454** is adapted for preventing data leaks. The additional data diodes **450a** and **450d** disposed prior to the respective checkers **452** and **454** are adapted to protect the integrity of the checkers, ensuring that they are not modified or compromised.

30 [0036] The data diode module **450** further comprises data diode gateways **430a** and **430b** disposed at the two terminating end of the data diode module **450**, one at each end respectively.

[0037] The reason that the checkers be placed between respective pair of data diodes so that the integrity of the checkers can be protected.

[0038] Each data diode gateway functions to simulate/emulate as an HTTP Server or Client to the connecting end such that the request-response sessions are carried out between the connecting end and the data diode gateway. In other word, as the data diode gateway on one side is receiving request/response (with/without payload) from the connecting end, that data diode gateway relays the received message to the other data diode gateway of the data diode module through the data diode and checker. The gist of the embodiment of the present invention is that within the data diode module channels the incoming data/message in a separate path from the outgoing data/message and process them separately, while enabling the request-response session which requires to be done in the same network connection between the same pair of IPEndpoints. It is achieved by using the data diode gateway to act/simulate as HTTP server/client to the sender on both connecting ends, and accordingly, one original request-response session is now becoming two request-response sessions. The data diode gateway is further adapted to map and manage the connections and sessions to ensure that all the request-response sessions are mapped and relayed to the correct corresponding connecting points.

20

[0039] FIG. 5 illustrates a flow chart of establishing request-response connections through a data diode network in accordance with one embodiment of the present invention. The method of establishing the request-response connection between two connecting ends having a data diode module deployed there between, at step 502. At step **504**, one connecting end, such as the client, may send a request to another receiving connecting end, such as the server, via the data diode module. The data diode gateway of the data diode module connected at one terminating end of the two independent connection paths receives the request from the connecting end.

[0040] At step **506**, the data diode gateway conveys the request to another data diode gateway of the data diode module connected at another terminating end of the two independent connection paths. At step **508**, the another data diode gateway sends a corresponding request to the receiving connecting end. At step **512**, the receiving

30

- connecting end responds to the another data diode gateway with a response. Up till now, a request-response connection is established between the receiving connecting end and the another data diode gateway. At step **514**, the another data diode gateway conveys the response to the data diode gateway through another independent connection path. At
- 5 step 516, the data diode gateway responds to the connecting end with a corresponding response. The corresponding response is responded to the original request from the original connecting end, thereby establishing a request-response connection between the data diode gateway with the original connecting end.
- 10 **[0041]** While specific embodiments have been described and illustrated, it is understood that many changes, modifications, variations and combinations thereof could be made to the present invention without departing from the scope of the invention.

Claims

1. A data diode module for establishing a request-response connection between a
5 client and a server as two connecting ends over a communication network, the data diode module comprising;

two independent connection paths, each having a data diode connected on each connection path forming a unidirectional transmission channel within the data diode module, the two data diodes are disposed in an opposing data direction;

10 two data diode gateways, each connected at a terminating end of the two independent connection paths, wherein the data diode gateways are adapted for mapping and managing connection end points in a manner that each of the data diode gateways emulates as an HTTP server or client to the respective connecting end to establish the request-response connection between the connecting end and the data diode gateway, the
15 data diode gateway on one side further conveys messages from the connecting end to the data diode gateway on another side.

2. The data diode module according to claim 1, wherein each independent connection path further comprises a checker for detecting and controlling network traffic
20 based on predetermined rules.

3. The data diode module according to claim 2, wherein the checker comprises any of a whitelist, Anti-virus scanner, static code scanner, machine learning antivirus, and input validation checker.
25

4. The data diode module according to claim 2, wherein the checker is disposed before the data diode on each independent connection path.

5. The data diode module according to claim 4, further comprises a second data
30 diode disposed before the checker on each independent connection path.

6. The data diode module according to claim 1, whereby the data diode module operationally receives a request from the connecting end, the data diode gateway receives and conveys the request to the another data diode gateway through one of the

independent connection paths, whereby the another data diode gateway sends a corresponding request to the receiving connecting end, and upon receiving the corresponding request at the receiving connecting end, the receiving connecting end sends a response to the another data diode gateway, thereby establish a request-response
 5 connection between the another data diode gateway and the receiving connecting end;
 and

wherein the another data diode gateway receives the response from the receiving connecting end and conveys the response to the data diode gateway through another one
 10 of the independent connection paths, the data diode gateway sends a corresponding response to the connecting end with the corresponding response, thereby establishing a request-response connection between the data diode gateway and the connecting end.

7. A data diode network adapting a data diode module of any one of the preceding
 15 claims.

8. A method for establishing request-response connections over a data diode network having a client and a server as two connecting ends, the method comprising:
 20 deploying a data diode module on the data diode network having two independent connection paths, each having a data diode connected on one independent connection path forming a unidirectional transmission channel within the data diode module, wherein the two data diode are disposed in an opposing data direction, the data diode module further comprises two data diode gateways, each connected at a terminating end
 25 of the two independent connection paths;

receiving, by a data diode gateway of the data diode module connected at one terminating end of the two independent connection paths, a request from one connecting end;

conveying the request to another data diode gateway of the data diode module
 30 connected at another terminating end of the two independent connection paths;

sending a corresponding request to the receiving connecting end;

responding, by the receiving connecting end, to the another data diode gateway with a response to establish a request-response connection between the another data diode gateway and the receiving connecting end;

conveying the response to the data diode gateway through another one of the
5 independent connection paths,

sending a corresponding response to the connecting end to establish a request-response connection between the data diode gateway and the connecting end.

9. The method according to claim 8, wherein the method is applicable over generic
10 TCP connections having data diode.

10. The method according to claim 9, wherein the data diode module of claim 1 is deployed.