

REIVINDICACIONES

1. Un sistema para suministrar una arquitectura de vínculo seguro múltiple (MSL), que comprende:

un componente de red privada virtual (VPN) MSL (104) que incluye primera lógica que, cuando se ejecuta por un procesador (930), hace que el sistema realice lo siguiente:

crear un primer túnel VPN entre una estación de trabajo de cliente (102) y una primera compuerta de propietario (120a);

enviar un datagrama de salida de la estación de trabajo de cliente (102) a la primera compuerta de propietario (120a);

recibir un datagrama de entrada desde la primera compuerta de propietario (120a) a la estación de trabajo de cliente (102), en donde el datagrama de entrada incluye una dirección de protocolo de internet (IP) fuente y una dirección de protocolo de internet (IP) destino que se configura a una dirección IP privada de propietario de VPN (104); y

enviar el datagrama de entrada con la dirección IP destino; y

un traductor de dirección de red (NAT) gemelo MSL que incluye segunda lógica que, cuando se ejecuta por el procesador (930), hace que el sistema realice por lo menos lo siguiente:

recibe el datagrama de entrada de VPN MSL (328);

registra una nueva dirección IP privada de propietario de VPN (104a) de la dirección IP fuente en el datagrama de entrada;

asigna una nueva dirección IP privada única (UPIP) para el datagrama de entrada y la estación de trabajo de cliente (102); y

envía el datagrama de entrada a la estación de trabajo de cliente (102),

en donde el sistema adicionalmente crea un segundo túnel VPN entre la estación de trabajo de cliente (102) y una segunda compuerta de propietario (102b) mientras se está utilizando el primer túnel VPN.

2. El sistema de la reivindicación 1, en donde la primera lógica además hace que el sistema realice lo siguiente:

 encripte el datagrama de salida y transfiera el datagrama de salida a la primera compuerta de propietario (120a); y

 reciba el datagrama de entrada en una forma encriptada de la primera compuerta de propietario (120a) y descifre el datagrama de entrada.

3. El sistema de la reivindicación 1, en donde la segunda lógica además hace que el sistema mapee una dirección UPIP en el datagrama de salida a una dirección IP privada.

4. El sistema de la reivindicación 1, que además comprende un componente de interfaz de usuario VPN MSL (114) que incluye tercera lógica que, cuando se ejecuta por el procesador (930), hace que el sistema suministre una interfaz de usuario para establecer el primer túnel VPN a la estación de trabajo de cliente (102).

5. El sistema de la reivindicación 1, que además comprende un componente de administración MSL (116) que incluye cuarta lógica que, cuando se ejecuta por el procesador (930), hace que el sistema cree el primer túnel VPN.

6. El sistema de la reivindicación 1, en donde la segunda lógica además hace que el sistema remita el datagrama de entrada a un componente de Proceso de Texto Claro limpio de estantería comercial (COTS) (226) para procesar el datagrama de entrada.

7. El sistema de la reivindicación 1, en donde el NAT gemelo MSL (110) y el VPN MSL (328) residen en la estación de trabajo de cliente (102) y en donde la estación de trabajo de cliente (102) además incluye un componente de interfaz de usuario VPN MSL (114) y un componente de administración de MSL (116).

8. El sistema de la reivindicación 1, que además comprende un servidor MSL (204), en donde el VPN MSL (328) y el NAT gemelo MSL (110) residen en el servidor MSL (204) que es remoto de la estación de trabajo de cliente (102), en donde el sistema además comprende un componente de interfaz de usuario VPN MSL (114), un primer componente VPN MSL (214), y un primer componente de administración de MSL (218) que reside en la estación de trabajo de cliente (102), y en donde el sistema además comprende un componente de proceso de texto claro limpio de estantería comercial (COTS) (226), un componente VPN COTS (224), y un segundo componente de administración de MSL (230) que reside en el servidor MSL (204).

9. El sistema de la reivindicación 1, que además comprende un enrutador de compuerta MSL (304) que incluye el VPN MSL (328) y el NAT gemelo MSL (110), en donde el sistema además comprende un primer componente VPN COTS (414), un componente de administración MSL (116) que reside en la estación de trabajo de cliente (102), y en donde el sistema además comprende un segundo componente VPN COTS (322) y un componente de administración de servidor MSL (438) que reside en el enrutador de compuerta MSL (304).

10. El sistema de la reivindicación 1, que además comprende un aparato MSL (404) y un servidor MSL (204), en donde el componente VPN MSL (439) y el NAT gemelo MSL (324) residen en el servidor MSL (204), en donde el sistema además comprende un primer componente VPN COTS (426) y un componente de interfaz de usuario VPN MSL (418) que residen en la estación de trabajo de cliente (102), en donde el

sistema además comprende un primer componente de administración de servidor MSL (438), un segundo componente VPN COTS (422), un tercer componente VPN COTS (426), y un componente de cliente de proceso de texto claro COTS (424) que reside en el aparato MSL (404), y en donde el sistema además comprende un segundo componente de administración de servidor MSL (230), un cuarto componente VPN COTS (432), y un segundo cliente de proceso de texto claro COTS (434) que reside en el servidor MSL (204).

11. El sistema de la reivindicación 1, que además comprende un centro de operaciones de red (NOC) MSL (504), en donde el NAT gemelo MSL (528) y el componente VPN MSL (531) residen en el NOC (504), en donde el sistema además comprende un cliente VPN COTS (514), un componente de interfaz de usuario VPN MSL (516), y un componente de administración de MSL (518) que reside en la estación de trabajo de cliente (102), y en donde el sistema además comprende un componente VPN COTS (524), un componente de proceso de texto claro COTS (526), un componente administrador de sesión (530), y un componente administrador de ingreso que reside en el NOC MSL (504).

12. Un método para suministrar una arquitectura de vínculo seguro múltiple (MSL), que comprende:

- crear un primer túnel VPN entre una estación de trabajo de cliente (102) y una primera compuerta de propietario (120a);

- enviar un datagrama de salida de la estación de trabajo de cliente (102) a la primera compuerta de propietario (120a);

- recibir un datagrama de entrada desde la primera compuerta de propietario (120a) a la estación de trabajo de cliente (102), en donde el datagrama de entrada incluye una dirección de protocolo de internet (IP) fuente

y una dirección de protocolo de internet (IP) destino que se configura a una dirección IP privada de propietario de VPN;

registrar una nueva dirección IP privada de propietario de VPN de la dirección IP fuente en el datagrama de entrada;

asignar una nueva dirección IP privada única (UIP) para el datagrama de entrada y la estación de trabajo de cliente (102); y

enviar el datagrama de entrada a la estación de trabajo de cliente (102),

en donde el sistema adicionalmente crea un segundo túnel VPN entre la estación de trabajo de cliente (102) y una segunda compuerta de propietario (120b) mientras se está utilizando el primer túnel VPN.

13. El método de la reivindicación 12, que además comprende:

encriptar el datagrama de salida y transferir el datagrama de salida a la primera compuerta de propietario (120a); y

recibir el datagrama de entrada en una forma encriptada de la primera compuerta de propietario (120a) y descifrar el datagrama de entrada.

14. El método de la reivindicación 12, que además comprende mapear una dirección UIP en el datagrama de salida a una dirección IP privada.

15 El método de la reivindicación 12, que además comprende suministrar una interfaz de usuario para establecer el primer túnel VPN a la estación de trabajo de cliente (102).

16. El método de la reivindicación 12, que además comprende crear el primer túnel VPN.

17. El sistema de la reivindicación 12, que además comprende remitir el datagrama de entrada a un componente de Proceso de Texto Claro limpio de estantería comercial (COTS) (226) para procesar el datagrama de entrada.

18. Un sistema para suministrar una arquitectura de vínculo seguro múltiple (MSL), que comprende:

un componente de red privada virtual (VPN) MSL (104) que incluye primera lógica que, cuando se ejecuta por dispositivo de computación (124a), hace que el dispositivo de computación (124a) realice al menos lo siguiente:

crear un primer túnel VPN entre una estación de trabajo de cliente (102) y una primera compuerta de propietario (120a);

enviar un datagrama de salida de la estación de trabajo de cliente (102) a la primera compuerta de propietario (120a);

recibir un datagrama de entrada desde la primera compuerta de propietario (120a) a la estación de trabajo de cliente (102), en donde el datagrama de entrada incluye una dirección de protocolo de internet (IP) fuente y una dirección de protocolo de internet (IP) destino que se configura a una dirección IP privada de propietario de VPN;

registrar una nueva dirección IP privada de propietario de VPN de la dirección IP fuente en el datagrama de entrada;

asignar una nueva dirección IP privada única (UPIP) para el datagrama de entrada y la estación de trabajo de cliente (102); y

enviar el datagrama de entrada a la estación de trabajo de cliente (102),

en donde el sistema adicionalmente crea un segundo túnel VPN entre la estación de trabajo de cliente (102) y una segunda compuerta de propietario (102b) mientras se está utilizando el primer túnel VPN.

19. El sistema de la reivindicación 18, en donde la lógica además hace que el dispositivo de computación realice por lo menos lo siguiente:

 encriptar el datagrama de salida y transferir el datagrama de salida a la primera compuerta de propietario (102a); y

 recibir el datagrama de entrada en una forma encriptada de la primera compuerta de propietario (102a) y descifrar el datagrama de entrada.