Amended claims according to Art. 19 PCT

CLAIMS

1. A device (10) for controlling a communication network (100) having a plurality of terminals (21 - 28) for a data communication, comprising:

a control unit (11) configured to decouple a data plane (L1) and a control plane (L2) of the data communication and to pro-actively modify at least one characteristic of the communication network (100) which is visible from the outside (200) of the communication network (100) during a communication session using the decoupled control plane (L2).

2. The device according to claim 1,
characterized in that
the control unit (11) is configured to pro-actively modify the communication network (100) such that different security zones having different security levels and/or different security functions are dynamically establishable in the communication network (100).

3. The device according to claim 1 or 2,
characterized in that
the control unit (11) is configured to change a virtual address of at least one of the plurality of terminals (21 -28) during the communication session using the decoupled control plane (L2).

4. The device according to claim 3,
characterized by

a random generator (19) for outputting a random value (ZW), wherein the control unit (11) is configured to change the virtual address depending on the random value (ZW) outputted by the random generator (19).

5. The device according to any one of the claims 1 or 4,
characterized in that
the control unit (11) is configured to modify the configuration of the communication network (100) during the communication session using the decoupled control plane (L2).

6. The device according to any one of the claims 1 or 5,
characterized in that
the control unit (11) is configured to modify a routing behavior of the communication network (100) during the communication session using the decoupled control plane (L2).

7. The device according to any one of the claims 1 or 6,
characterized in that
the control unit (11) is configured to modify at least one application of the communication network (100) and/or a port mapping of the at least one application during the communication session using the decoupled control plane (L2).

8. The device according to any one of the claims 1 or 7,
characterized in that
the control unit (11) is configured to exchange a first crypto-algorithm employed by the communication network (100) with a second crypto-algorithm during the communication session.

9. The device according to any one of the claims 1 or 8,
characterized in that

the control unit (11) is configured to modify a data pattern of the communication network (100), particularly a payload data profile of at least one of the terminals (21 - 28).

10. The device according to any one of the claims 1 or 9,
characterized in that
the communication session includes a plurality of transactions of data, wherein the control unit (11) is configured to modify the at least one characteristic of the communication network (100), which is visible from the outside (200) of the communication network (100), after a subset of the plurality of transactions.

11. The device according to any one of the claims 1 or 10,
characterized in that
the communication session includes a plurality of transactions of data, wherein the control unit (11) is configured to modify the at least one characteristic of the communication network (100), which is visible from the outside (200) of the communication network (100), after each one of the plurality of transactions.

12. The device according to any one of the claims 1 or 11,
characterized in that
the control unit (11) is configured to decouple the control plane (L1) and the data plane (L2) of the data communication using software-defined-networking.

13. The device according to any one of the claims 1 or 12,
characterized by
a random generator (19) that is coupled to the control unit (11) and configured to randomly trigger the control unit (11) for modifying the at least one characteristic, which is visible from the outside (200) of the communication network

(100), at least once during the communication session, more particularly several times during the communication session.

14. The device according to any one of the claims 1 or 13,
characterized by

a first protection unit (15) for detecting, isolating, and antagonizing accesses from non-authorized entities on the communication network (100).

15. The device according to claim 14,
characterized by

a second protection unit (16) for warning and alerting a determination system (300) which is coupleable to the device (10).

16. The device according to claim 14 or 15,
characterized by

a third protection unit (17) for restoring at least one critical network function.

17. The device according to any one of the claims 1 or 16,
characterized by

an analyzing unit (12) for providing analyzing data during accesses on the communication network (100) from non-authorized entities.

18. The device according to claim 17,
characterized by

a data determination unit (14) for determining status data using the provided analyzing data, the status data being suitable particularly for specifying a security situation of the communication network (100).

19. The device according to claim 18,
characterized by
an interface unit (20) for transmitting the status data to a determination system (300) which is couplable to the device (10).

20. The device according to any one of the claims 1 or 19,
characterized in that
the communication network (100) comprises an infrastructure of layers that are stacked on one another, wherein the control unit (11) is implemented as a virtual overlay network overlaying a layer-2 and a layer-3 of the infrastructure.

21. The device according to any one of the claims 1 or 20,
characterized in that
the device (10) uses a combination of a security protocol and a tunneling-protocol.

22. A router (30) for a communication network (100) which incorporates a device (10) according to any one of the claims 1 to 21.

23. A switch (40) for a communication network (100) which incorporates a device (10) according to any one of the claims 1 to 21.

24. A firewall (50) for a communication network (100) which incorporates a device (10) according to any one of the claims 1 to 21.

25. A communication network (100), comprising:
a plurality of terminals (21 - 28) for data communication, and
a device (10) for controlling the communication network (100) according to any one of the claims 1 to 21.

26. A method for controlling a communication network (100) having a plurality of terminals (21 - 28) for data communication comprising the steps of:

decoupling (901) of a data plane (L1) and a control plane (L2) of the data communication, and

pro-actively modifying (902) at least one characteristic of the communication network (100) which is visible from the outside (200) of the communication network (100) during a communication session using the decoupled control plane (L2).

27. A computer program product which causes the execution of the method according to claim 26 on a program controlled unit.

Claims

1. A device for controlling a communication network having a plurality of terminals for a data communication, comprising:

a control unit configured to decouple a data plane and a control plane of the data communication and to pro-actively modify at least one characteristic of the communication network which is visible from the outside of the communication network during a communication session using the decoupled control plane.

2. The device according to claim 1,
characterized in that
the control unit is configured to pro-actively modify the communication network such that different security zones having different security levels and/or different security functions are dynamically establishable in the communication network.

3. The device according to claim 1 or 2,
characterized in that
the control unit is configured to change a virtual address of at least one of the plurality of terminals during the communication session using the decoupled control plane.

4. The device according to claim 3,
characterized by

a random generator for outputting a random value, wherein the control unit is configured to change the virtual address depending on the random value outputted by the random generator.

5. The device according to any one of the claims 1 or 4,
characterized in that
the control unit is configured to modify the configuration of the communication network during the communication session using the decoupled control plane.

6. The device according to any one of the claims 1 or 5,
characterized in that
the control unit is configured to modify a routing behavior of the communication network during the communication session using the decoupled control plane.

7. The device according to any one of the claims 1 or 6,
characterized in that
the control unit is configured to modify at least one application of the communication network and/or a port mapping of the at least one application during the communication session using the decoupled control plane.

8. The device according to any one of the claims 1 or 7,
characterized in that
the control unit is configured to exchange a first crypto-algorithm employed by the communication network with a second crypto-algorithm during the communication session.

9. The device according to any one of the claims 1 or 8,
characterized in that
the control unit is configured to modify a data pattern of the communication network, wherein the data pattern of the communication network includes a payload data profile of at least one of the terminals.

10. The device according to any one of the claims 1 or 9,
characterized in that
the communication session includes a plurality of transactions of data, wherein the control unit is configured to modify the at least one characteristic of the communication network, which is visible from the outside of the communication network, after a subset of the plurality of transactions.

11. The device according to any one of the claims 1 or 10,
characterized in that
the communication session includes a plurality of transactions of data, wherein the control unit is configured to modify the at least one characteristic of the communication network, which is visible from the outside of the communication network, after each one of the plurality of transactions.

12. The device according to any one of the claims 1 or 11,
characterized in that
the control unit is configured to decouple the control plane and the data plane of the data communication using software-defined-networking.

13. The device according to any one of the claims 1 or 12,
characterized by
a random generator that is coupled to the control unit and configured to randomly trigger the control unit for modifying the at least one characteristic, which is visible from the outside of the communication network, at least once during the communication session.

14. The device according to any one of the claims 1 or 13,
characterized by
a first protection unit for detecting, isolating, and antagonizing accesses from non-authorized entities on the communication network.

15. The device according to claim 14,
characterized by
a second protection unit for warning and alerting a determination system which is coupleable to the device.

16. The device according to claim 14 or 15,
characterized by
a third protection unit for restoring at least one critical network function.

17. The device according to any one of the claims 1 or 16,
characterized by
an analyzing unit for providing analyzing data during accesses on the communication network from non-authorized entities.

18. The device according to claim 17,
characterized by
a data determination unit for determining status data using the provided analyzing data, the status data being suitable for specifying a security situation of the communication network.

19. The device according to claim 18,
characterized by
an interface unit for transmitting the status data to a determination system which is coupleable to the device.

20. The device according to any one of the claims 1 or 19,
characterized in that
the communication network comprises an infrastructure of layers that are stacked on one another, wherein the control unit is implemented as a virtual overlay network overlaying a layer-2 and a layer-3 of the infrastructure.

21. The device according to any one of the claims 1 or 20,
characterized in that
the device uses a combination of a security protocol and a tunneling-protocol.

22. A router for a communication network which incorporates a device according to any one of the claims 1 to 21.

23. A switch for a communication network which incorporates a device according to any one of the claims 1 to 21.

24. A firewall for a communication network which incorporates a device according to any one of the claims 1 to 21.

25. A communication network, comprising:
a plurality of terminals for data communication, and
a device for controlling the communication network according to any one of the claims 1 to 21.

26. A method for controlling a communication network having a plurality of terminals for data communication comprising the steps of:
decoupling of a data plane and a control plane of the data communication, and
pro-actively modifying at least one characteristic of the communication network which is visible from the outside of the communication network during a communication session using the decoupled control plane.

27. A computer program product which causes the execution of the method according to claim 26 on a program controlled unit.