~~[DESCRIPTION]~~

~~[Title]~~

COMMUNICATION SYSTEM, POLICY MANAGEMENT APPARTATUS, COMMUNICATION METHOD, AND PROGRAM

[Technical Field]

[0001]

(CROSS-REFERENCE TO RELATED APPLICATIONS)

The present invention is based upon and claims the benefit of the priority of Japanese Patent Application No. 2011-204487 (filed on September 20, 2011), the disclosure of which is incorporated herein in its entirety by reference.

[0002]

The present invention relates to a communication system, a policy management apparatus, a control method, and a program. More specifically, the invention relates to a communication system, a policy management apparatus, a communication method, and a program for implementing communication by forwarding a packet using a forwarding node disposed on a network.

[Background]

[0003]

Patent Literature (PTL) 1, Non Patent Literatures (NPLs) 1 and 2 describe a technology referred to as OpenFlow (OpenFlow). In the OpenFlow, communication is regarded as an end-to-end flow, and path control, failure recovery, load distribution, and path optimization are performed on a per-flow basis.

[0004]

An OpenFlow switch specified in Non Patent Document 2 includes a secure channel for communication with an OpenFlow controller corresponding to a control apparatus. The OpenFlow switch operates according to a flow table in which appropriate adding or rewriting is instructed by the OpenFlow controller.

[0005]

In the flow table, a set of a matching rule (header fields) to be matched against a packet header, flow statistics information (counters),

and actions defining processing content is defined for each flow (refer to Fig. 3).

[0006]

When the OpenFlow switch receives a packet, the OpenFlow switch searches the flow table for an entry having a matching rule that matches header information of the received packet (refer to the header fields in Fig. 3).

[0007]

When the entry that matches the received packet is found as a result of the search, the OpenFlow switch updates the flow statistics information (one or more counters), and executes processing content (e.g., transmission of the packet from a specified port, flooding of the packet, discarding of the packet, or the like) described in the action field of the entry.

[0008]

On the other hand, when the entry that matches the received packet is not found as a result of the search, the OpenFlow switch forwards the received packet to the OpenFlow controller through the secure channel, and requests the OpenFlow controller to determine a path of the packet, based on the transmission source and the transmission destination of the received packet. The OpenFlow switch receives a flow entry for implementing forwarding of the packet according to this path, and then updates the flow table.

[0009]

In this manner, the OpenFlow switch performs packet forwarding by using an entry stored in the flow table as a processing rule.

~~[Citation List]~~

~~[Patent Literature]~~

[0010]

[PTL 1]

International Publication No. WO2008/095010

~~[Non-Patent Literature]~~

[0011]

[NPL 1]

Nick McKeown and seven other authors, "OpenFlow: Enabling Innovation in Campus Networks," March 14, 2008 [on line], [Searched on September 7, 2011], Internet <URL: http://www.openflowswitch.org/documents/openflow-wp-latest.pdf>.

[NPL 2]

"OpenFlow Switch Specification, Version 1.1.0 Implemented (Wire Protocol 0x02)," February 28, 2011, [online], [Searched on September 7, 2011], Internet <URL: http://www.openflowswitch.org/documents/openflow-spec-v1.1.0.pdf>.

[Summary]

~~[Technical Problem]~~

[0012]

Each disclosure of the above-listed Patent Literature and Non Patent Literatures is incorporated herein by reference thereto. The following analysis is made by the present invention.

[0013]

The OpenFlow controller or the controller in the OpenFlow described in Patent Literature 1 performs a permission check by referring to an access control rule when a new flow is generated. Then, the OpenFlow controller performs access control by calculating the path (refer to [0052] in Patent Literature 1).

[0014]

The access control rule to be referred to when the new flow is generated is herein updated by receipt of an access control list (ACL: Access Control List) generated by a policy management apparatus.

[0015]

When the policy management apparatus generates the ACL, information on the host of an access source and information on the network resource of an access destination are needed.

[0016]

Even if a network administrator or a user who demands the access control manually supplies these pieces of information to the policy management apparatus, the access control can be performed. However, it takes much time and effort for the network administrator

Even if the network administrator or the user who demands the access control manually supply these pieces of information to the policy management apparatus, the access control can be performed. However, by this method, it takes much time and effort for the network administrator or the user to perform the access control. Consequently, it becomes difficult to perform the access control in the large-sized network or in the environment where the connection state of the host or the network resource frequently changes.

[0023]

Assume that the operation of specifying these pieces of information be semi-automated by the system, on the other hand. Then, if there could be provided to the network administrator or the user an abstract and easily comprehensible specifying method that will automatically follow a change once these pieces of information have been specified, by this semi-automation, the time and effort to be expended by the network administrator or the user could be greatly reduced. In this case, it would become possible to perform the access control in the large-sized network or in the environment where the connection state of the host or the network resource frequently changes, with the time and effort saved in a simple and practical way.

[0024]

However, in order to achieve the solution as described above, there is needed a function of collecting the current connection state of the host of the access source or information on the network resource of the access destination in real time and searching out information on a specific host or a specific network resource based on an abstract specification described in the access control policy.

[0025]

Then, there is a need that access control can be updated in real time even if there are a lot of devices and connection states of the devices frequently change or even if there are a lot of users and connection states of the users frequently change. ~~It is an object of the present invention to provide a communication system, a policy management apparatus, a communication method, and a program that~~

~~contribute to such a need.~~

~~[Solution to Problem]~~

[0026]

According to a first aspect of the present invention, there is provided a communication system, comprising:

a plurality of forwarding node processing a packet according to a processing rule;

a control apparatus that controls the plurality of forwarding nodes;

an authentication apparatus that authenticates a user who uses a host connected to one of the plurality of forwarding nodes; and

a policy management apparatus that includes at least one of (a) a first linking means that links an identifier of a host to be subject to access control and an identifier of a forwarding node to which the host is connected and (b) second linking means that links an identifier of a host to be subject to access control and an identifier of a user who uses the host, the policy management apparatus holding an access control policy for identifying a host to be subject to the access control using at least one of the identifier of the forwarding node and the identifier of the user, wherein

each of the plurality of forwarding nodes transmits to the policy management apparatus a set of an identifier of a host connected to own forwarding node and an identifier of the own forwarding node;

the authentication apparatus transmits to the policy management apparatus a set of an identifier of a host connected to one of the plurality of forwarding nodes and an identifier of a user,

the policy management apparatus refers to the access control policy and, if a host connected to one of the plurality of forwarding nodes is a host to be subject to the access control, notifies content of the access control to the control apparatus as an access control list, and

the control apparatus generates a processing rule in accordance with the access control list and sets the generated processing rule in the plurality of forwarding nodes.

[0027]

According to a second aspect of the present invention there is

the access control and an identifier of a user who uses the host;

receiving from each of the plurality of forwarding nodes a set of an identifier of a host connected to own forwarding node and an identifier of the own forwarding node;

receiving from the authentication apparatus a set of an identifier of a host connected to one of the plurality of forwarding nodes and an identifier of a user; and

referring to the access control policy and, if the host connected to one of the plurality of forwarding node is the host to be subject to the access control, notifying to the control apparatus content of the access control as the access control list.

~~[Advantageous Effects of the Invention]~~

[0031]

The present invention provides the following advantage, but not restricted thereto. According to the communication system, the policy management apparatus, the communication method, and the program, even if there are a lot of devices and connection states of the devices frequently change, or even if there are a lot of users and connection states of the users frequently change, it becomes possible to update access control in real time.

[Brief Description of Drawings]

[0032]

[Fig. 1]

Fig. 1 is a block diagram showing a configuration of a communication system according to an exemplary embodiment, as an example.

[Fig. 2]

Fig. 2 is a sequence diagram showing an operation of the communication system according to the exemplary embodiment, as an example.

[Fig. 3]

Fig. 3 is a diagram showing a configuration of an entry stored in an OpenFlow flow table (in Non Patent Literature 2).

[~~Description of Embodiments~~Preferred Modes]

[0033]

In the present disclosure, there are various possible modes, which include the following, but not restricted thereto. First, an overview of the present disclosure will be described.