A sub-network (12) is coupled to the Internet (10) via a firewall (23). Identifier based access policy rules are provided for devices and/or services coupled to the sub-network. The identifiers are statically assigned to devices (14) coupled to the sub-network (12) and/or to services provided by said devices (14). Network addresses are dynamically assigned to the devices, for example by means of a DHCP server. A firewall management unit monitors messages on the sub-network (12) to detect messages that associate the identifiers with network addresses assigned to devices (14) assigned to the identifiers. The firewall management unit dynamically redefines firewall rules expressed in terms of the network addresses obtained by said monitoring, dependent on the access policy rules for the identifiers assigned to the devices and/or services for which the network addresses obtained by said monitoring are used. Preferably, the firewall is located between a tunnel endpoint for a virtual private network and the sub-network, the firewall being initialized to block all messages for network addresses in a dynamically assignable range, the firewall management unit making some rules more permissive when a network address for a device has been determined.
Dynamic firewall rule definition

The networks like the Internet allow interconnection of many private (sub-)networks. By means of tunneling different sub-networks can be coupled to form a virtual private network, wherein the devices from these different sub-networks can send messages to each other as if they were connected to a single private network. "Tunneling" means that messages are transmitted via the Internet (or other interconnecting networks) in a way wherein the addresses of the messages that are used in the sub-networks are not used as address during transmission via the Internet. A virtual private network is realized for example by coupling each sub-network to the Internet via a residential gateway. In each sub-network messages with destination addresses for devices in the other sub-network are detected and transmitted over the Internet between the residential gateways of the sub-networks, inserted in messages addressed to the residential gateway of the other sub-network. The residential gateway of the other sub-network, in turn, forwards the messages to devices connected to the other sub-network.

Preferably firewalls are used at the residential gateways to block selected messages. A firewall is conventionally implemented to apply a set of rules, in terms of source and destination addresses of messages that must be blocked and the types of messages that must be blocked.

Network addresses are often assigned dynamically to devices in a sub-network. In one example this is done by a so-called DHCP (Dynamic Host Configuration Protocol) server. Such a server manages a range of available addresses and assigns addresses from this range to devices upon request from the devices. In this way the address of a particular device may be different at different times, for example after the device has been switched off and on again. Usually, the sub-network contains only one, or very few devices with a static address that does not change, the remaining devices in the sub-network having dynamically changing addresses. Thus, for example, the residential gateway or a central computer of the sub-network may have a static address and printers etc. in the sub-network may have dynamically changing addresses.

Dynamic network address assignment to devices complicates management of firewalls. In a simple solution the firewall rules can account for dynamic network address
assignment by blocking out messages to or from the whole range of available addresses of
the DHCP server. Thus, for example messages from devices in a first sub-network to devices
with dynamically assigned addresses in a second sub-network could all be passed if the first
and second sub-network form a virtual private sub-network, or blocked if not. In addition,
specific firewall rules could be defined for those network addresses that are statically
assigned to devices to provide selective access.

US patent No 6,678,827 describes a system for remote management of
firewalls. Security policy templates are defined, which express abstract firewall rules in terms
of abstract services instead of network addresses. In addition network profiles are defined
which identify network addresses associated with an abstract service. Concrete instantiations
of firewall rules are made by substituting the network addresses from the network profile into
the security policy templates. The user must generate the network profile. This would be very
cumbersome if access rules would be different for different individual dynamically assigned
network addresses.

US patent application no 2004/0249907 describes a technique for discovering
devices or services in a (sub-) network. Discovered devices or services are selected to
perform various services and the user is prompted to configure the devices or services. One
of the services that can be configured in this way by the user is the DHCP service.

European Patent Application No. 1313290 describes a firewall for a laptop
computer, which changes between different sets of firewall rules dependent on a detected
network address of the laptop, which is taken to be indicative of whether the laptop is
coupled to a safe, closed network or an open network.

Among others, it is an object of the invention to provide for a method of
communicating with a sub-network using a firewall when dynamic address assignment is
used.

A firewall policy management apparatus according to claim 1 is provided. The
firewall policy management unit redefines a firewall rule of a firewall coupled between a
communication network and a sub-network dynamically. The redefined firewall rules are
expressed in terms of the network addresses. The redefined firewall rules are derived from
access policy rules that are expressed in terms of identifiers. Network addresses are assigned
dynamically, and the firewall rules are generated after detection of dynamic associations between identifiers and network addresses. Thus, automatic, dynamic firewall reconfiguration is realized.

In an embodiment the firewall is configured to apply the redefined rules to messages received through a virtual private network tunnel, and preferably only to such messages, for example after extracting messages from tunnel messages that have been transmitted through an open communicating network and before injection into the sub-network, or as part of extraction. Thus, virtual private networks with adaptive rules can be realized.

In an embodiment a plurality of virtual private network tunnels through the communication network to the sub-network is serviced, the firewall policy rules differentiating between different ones of the tunnels. Thus, for example more and less virtual private networks can be supported.

Preferably the firewall initially blocks all messages to devices with network addresses within a range of network addresses that are available for dynamic assignment in the sub-network, the redefined firewall rules allowing at least selected messages to pass through the firewall when these messages have a destination address to a particular one of the devices. In a further embodiment the redefined rules are undone when the device signs off, or nothing is heard from a device during a time out interval. Thus, permissive firewall rules are established only when a device or service is active, avoiding that messages can get through when a network address is reassigned to a device that should be shielded off by the firewall.

These and other objects and advantages will become apparent from a description of exemplary embodiments, by reference to the following figures.

Fig. 1 shows a networked system,
Fig. 2 shows a firewall policy management device,
Fig. 3 shows a flow-chart of firewall policy management,
Fig. 4 shows a firewall policy management device,
Fig. 5 shows a firewall policy management device.

Figure 1 shows a networked system. The system comprises a main network interconnection circuitry 10 (e.g. the Internet) and a plurality of sub-networks each with its
own sub-network interconnection circuitry 12 and a number of devices 14,16 (only some referenced explicitly by way of example) coupled to the sub-network interconnection circuitry 12. It should be understood that "interconnection circuitry" as is used herein includes to refer to both wired and/or wireless connections, as well as optical connections and associated devices for transporting and routing messages if present. The devices 14, 16 in each sub-network include a gateway device 16 coupled between the main network interconnection circuitry 10 and the sub-network interconnections 12.

In operation devices 14, 16 transmit messages via interconnections 10, 12. Each message typically contains a destination address, which identifies a receiving device 14, 16 for which the message is destined.

Part of the devices 14, 16, for example the gateway devices 16, may have predetermined globally unique addresses, selected so that no other device 14, 16 coupled to main network interconnections 10 has the same address. In the Internet (IP version 4) environment, such addresses are typically represented as a series of four numbers separated by dots. Another part of the devices 14, 16 are locally assigned devices 14, 16 that have locally assigned addresses, which are assigned to the locally assigned devices 14, 16 by an assigning device.

Messages with locally assigned addresses of devices 14, 16 that are connected to the sub-network interconnections 12 of the sub-network wherein these messages are initially transmitted are detected by these devices 14, 16 and received. Messages addressed to devices 14, 16 with a globally unique address on main network interconnections 10 are forwarded by gateway device 16 to their destination.

In addition, virtual networks may be defined, wherein at least a first and second one of the sub-networks are coupled. Information about such virtual networks may be stored for example in gateway device 16 of the sub-networks that are part of such a virtual network. The information may include for example a list of addresses of devices 14, 16 in the other sub-network, or an identification of one or more ranges of addresses reserved for such devices. When a message is detected in the first network that has a locally assigned address addressed to a device 14, 16 in the second sub-network, gateway device 16 of the first sub-network transmits the message to the second sub-network. Typically such a message is encapsulated in a further message that is addressed to a device (e.g. the gateway device 16) in the second sub-network that has a globally unique address. In the second network the message is converted back to the original message with its locally assigned address. These messages are then detected by local devices 14, 16 and received.
Local assignment of addresses may be performed for example by the gateway device 16 that is connected between the locally assigned device 14, 16 and the main network interconnections 10. Alternatively, another device 14, 16 (e.g. a main computer) coupled to the sub-network interconnections 12 may be used, or even a remote device coupled to sub-network interconnections 12 via main interconnections 12. The locally assigned addresses may be assigned dynamically, each time when a device 14, 16 starts up, or more persistently, for example each time a device 14, 16 is added to sub-network interconnections 12 of a sub-network.

In operation gateway device 16 provides a firewall service. That is, gateway device 16 inspects messages passing from main network 10 to its corresponding sub-network 12 and blocks transmission of selected messages dependent on whether the transmission is permitted by firewall rules.

Figure 2 shows a functional structure of a gateway device 16 that acts as firewall policy management device. Although different units are distinguished in the functional structure, which may correspond to respective hardware circuits, it should be appreciated that alternatively, some or all of the different units may correspond to the same hardware circuits, when executing different programs, or executing the same program in different configurations. Gateway device 16 is coupled between a first connection 28 to a closed local network (e.g. a sub-network 12 not shown) and a second connection 29 to an open network (e.g. main network 10 not shown).

Gateway device 16 comprises a firewall implementation unit 23 coupled to the network connections 28, 29 via respective interface units 21, 25. In addition gateway device 16 comprises a firewall policy management unit 24 coupled to the network connection 28 to the closed local network via a network interface 22 and a storage unit 26.

Interface unit 25 between firewall implementation unit 23 and second connection 29 is preferably a virtual private network tunnel endpoint, which translates messages from second connection 29 that contain virtual private network messages into messages for transmission on the closed local network via first connection 28. These messages are filtered by firewall implementation unit 23, which allows only those messages to pass for which this is allowed by firewall rules. Conversely, the virtual private network tunnel endpoint preferably also translates messages from first connection 28 to messages for transmission to another tunnel endpoint via first connection 29 and the open network.

Storage unit 26 stores a set of access policy rules in terms of service identifiers or UUIDs of devices that may be actively coupled to the first connection 28 for the closed local network.
The access policy rules specify for example whether messages to all or part of these devices should be passed, optionally dependent on the source of the message or a sub-network that contains the source of the message. Similarly, the access policy rules may specify whether messages from devices should be passed, optionally dependent on the destination of the message or a sub-network that contains the destination of the message.

Figure 3 shows a flow-chart of operation of firewall policy management unit 24. In a first step 31 firewall policy management unit 24 listens for messages in the closed, local network that is connected to first connection 28. When a message is received firewall policy management unit 24 tests in a second step 32 whether the received message is an advertisement message. This is repeated from first step 31 until firewall policy management unit 24 detects an advertisement message.

Advertisement messages serve to discover devices that are actively coupled to the closed, local network that is connected to first connection 28. This may be done for example by monitoring messages on first connection 28 to detect SSDP service advertisements. The SSDP (Simple Search and Discovery Protocol) is a protocol wherein service advertisement messages are transmitted by devices 14 connected to the local network. A service advertisement message contains a network address (which may include a port number) and a service identifier.

Alternatively, or in addition to listening for advertisement messages, firewall policy management unit 24 may multicast search messages for eliciting responses with this information from actively connected devices that perform specified services.

When firewall policy management unit 24 has detected an advertisement message, firewall policy management unit 24 executes a third step 33 to check whether storage unit 26 contains an access policy rule for the advertised service. If so firewall policy management unit 24 executes a fourth step 34 wherein firewall policy management unit 24 updates a firewall rule for the network address from the advertisement message according to the access policy rule that has been found in storage unit 26.

In an embodiment network addresses are defined by a DHCP (Dynamic Host Control Protocol) server device coupled to the local network. Such servers are known per se.

Each time when a device without a permanent network address switches on, it sends a request for a network address to the DHCP server device. In response the DHCP server device selects an unused address from a reserved range and supplies this address in response to the request. When the device without a permanent network address switches off it transmits a "byebye" message, which enables the DHCP server to reuse its network address.
Preferably, the added rules are enabling rules, which allow firewall implementation unit 23 to pass selected messages to the network address. Also firewall implementation unit 23 is preferably initially programmed with access rules to block all messages addressed to an unassigned address. Thus, when the DHCP server device assigns a network address to a device, firewall implementation unit 23 will initially block all messages to that network address. Only after firewall policy management unit 24 has updated the firewall rules selected messages may be passed. As an alternative, some initial firewall access rules may be permissive (pass selected types of messages) and the updates by firewall policy management unit 24 may cause some of these types of messages to be blocked. However, it will be noted that this may entail the risk that some undesirable messages slip through initially.

In an embodiment firewall policy management unit 24 also listens for the "byebye" messages. In response to a "byebye" message firewall policy management unit 24 determines which firewall rules were changed, added or removed upon discovery of the device that has sent the "byebye" message and changes back, removes or reinstates these rules in response to the "byebye" message.

In a further embodiment firewall policy management unit 24 keeps time-out information for each of the devices for which firewall access rules have been changed, added or removed. The time out information is for each particular device is updated each time when a message from that device is detected (e.g. by writing a time value representative of the time of detection; alternatively the time out information may be a count value that is periodically incremented and reset upon detection). In this further embodiment firewall policy management unit 24 tests which time-out information has not been updated for a predetermined time and, if so, changes back, removes or reinstates these rules as if a "byebye" message was received.

It should be appreciated that the use of SSDP is only one example of detection of devices associated with network addresses. Furthermore, although an example has been given wherein service identifiers were used it should be appreciated that alternative device identifiers may be used, such as UUIDs (Universal Unique IDentifiers of devices). In this case, once a device is discovered firewall policy management unit 24 finds its network address and its device identifier, looks up access policy rules associated with the device identifier an programs firewall access rules into firewall implementation unit 23 for the associated network address. Furthermore, although use of a general discovery such as SSDP has been described, combined with DHCP address issuing, it should be appreciated that
alternatively a form of discovery linked to address issuing may be used, for example involving triggering of queries for device ID’s in response to requests for network addresses. This may simplify discovery of associations between a network addresses and an ID.

Various types of access policy rules may be used. The access policy rules may depend on the destination service and/or the device identifier and/or message type and/or message source address. In a simple embodiment, each access policy rule depends only on the destination service or the device identifier and the message type. In a more advance embodiment the rules are also dependent on the source address. Thus for example, messages form sub-networks 12 that form a virtual private network with a local network may passed selectively. In one embodiment, firewall implementation unit 23 and the tunnel endpoint are integrated and firewall implementation unit 23 is configured to perform the source dependent filtering dependent on the source address of the message that contains a tunneled message, in combination with a dependence on the type of the tunneled message and its destination network address.

Figure 4 shows a further functional structure of a gateway device 16 that acts as firewall policy management device. Herein a tunnel endpoint 40 and a general firewall unit 42 have been added. Tunnel endpoint 40 is coupled between the network interface 25 to the open network and firewall implementation unit 23. General firewall unit 42 is coupled between the network interface 25 to the open network and the network interface 21 to the closed network in parallel with the series arrangement of tunnel endpoint 40 and firewall unit 42. In operation, tunnel endpoint 40 received messages that contain tunneled messages, extracts the tunneled messages including a destination address and outputs the tunneled messages to firewall implementation unit 23. Firewall implementation unit 23 then blocks these messages according to rules defined by firewall policy management unit 24. Thus, for example, similar messages from different other sub-networks that form virtual private networks with the local network may be passed or blocked dependent on the range of addresses used by the other sub-networks. Messages that do not contain tunneled messages are supplied to general firewall unit 42 which blocks or passes these messages according to user defined or predetermined rules for example.

Figure 5 shows a further functional structure of a gateway device 16 that acts as firewall policy management device. Herein a tunnel endpoint 40 has been added. Tunnel endpoint 40 operates as a device coupled to the local sub-network via a network interface 51. Tunnel endpoint 40 receives messages from the open network, preferably via a gateway firewall (not shown) and the local network. Tunnel endpoint 40 extracts virtual private
network messages from the received messages and applies these virtual private network messages to firewall implementation unit 23. Firewall implementation unit 23 blocks these extracted messages according to rules defined by firewall policy management unit 24. Thus, messages for the virtual private network are selectively blocked by firewall implementation unit 23.

As has been mentioned the functional structure used in figures 2, 4 and 5 may be implemented by using different circuits for respective functional parts in these figures. Dedicated circuits or programmable circuits programmed to perform the described functions may be used. Alternatively, some functional parts may be integrated with one another.

Furthermore, although an embodiment has been shown wherein all parts are integrated in a residential gateway 16, it should be appreciated that alternatively some parts may be implemented in different devices that are coupled to each other via the local network. For example, the firewall policy management unit 24 may be implemented in a device separate from residential gateway 16 and the same goes for storage unit 26. A plurality of storage units may even be used to store different access policy rules.

Although an embodiment has been described wherein incoming messages for a virtual private network are filtered, it should be understood that filtering with rules defined by firewall policy management unit 24 may also be applied to incoming messages in general. Also, firewall unit may be designed to block outgoing messages dependent on rules defined by firewall policy management unit 24. In this case the access policy rules in storage unit 26 preferably include access policy rules specified in terms of types of source service and/or source device ID. In this case, firewall policy management unit 24 uses a discovered association between a network address and a source service type or device ID to generate firewall outward rules wherein the discovered network address is substituted.
CLAIMS:

1. A firewall policy management apparatus for redefining firewall rules in a firewall (23) functionally coupled between a communication network (10) and a sub-network (12), the firewall policy management apparatus comprising:
   - a sub-network interface (22) for coupling to the sub-network (12);
   - a storage arrangement (26) storing identifier based access policy rules expressed using identifiers assigned to devices (14) coupled to the sub-network (12) and/or services performed by said devices (12);
   - a message processing circuit (24) coupled to the sub-network interface (21) and the storage arrangement (26) and configured to monitor messages from the sub-network (12) to detect messages that associate the identifiers from the access policy rules with network addresses assigned to devices (14) assigned to the identifiers, the message processing circuit (24) being configured to dynamically redefine firewall rules expressed in terms of the network addresses obtained by said monitoring, dependent on the access policy rules for the identifiers assigned to the devices and/or services for which the network addresses obtained by said monitoring are used.

2. A firewall policy management apparatus according to claim 1, comprising the firewall (23), functionally coupled between the communication network (10) and the sub-network (12), the message processing circuit (24) being coupled to the firewall (23) for performing said redefining.

3. A firewall policy management apparatus according to claim 2, comprising a tunnel endpoint (40) for a virtual private network tunnel through the communication network (10) to the sub-network (12), the firewall (23) being configured to apply the redefined firewall rules to messages received through said virtual private network tunnel.

4. A firewall policy management apparatus according to claim 3, wherein the firewall (23) is configured to apply the redefined firewall rules only to messages received via said tunnel.
5. A firewall policy management apparatus according to claim 3, wherein the
tunnel endpoint (40) is configured to service a plurality of virtual private network tunnels
through the communication network (10) to the sub-network (12) from respective further
sub-networks (12), the firewall policy rules differentiating between different ones of the
further sub-networks (12), the message processing circuit (24) being configured to redefine
firewall rules to allow at least selected messages from a first part of the further sub-networks
(12) but not from a second part of the further sub-networks (12) to pass through the firewall
(23) when these messages have a destination address to a particular one of the devices.

6. A firewall policy management apparatus according to claim 2, wherein the
firewall (23) is configured to initially block all messages to devices with network addresses
within a range of network addresses that are available for dynamic assignment in the sub-
network (12), the message processing circuit (42) being configured to redefine firewall rules
to allow at least selected messages to pass through the firewall (23) when these messages
have a destination address to a particular one of the devices.

7. A firewall policy management apparatus according to claim 1, wherein the
message processing circuit (24) is configured to further monitor messages on the sub-network
(12) to detect a sign-off message from a particular one of the devices (14) and to undo
redefinitions of the firewall rules for involving the network address of said particular one of
the devices (14) in response to detection of the sign-off message.

8. A firewall policy management apparatus according to claim 1, wherein the
message processing circuit (24) is configured to maintain time-out information,
representative of durations of time intervals elapsed since respective ones of the devices (14)
were last heard of on the sub-network (12) and to undo redefinitions of the firewall rules for
involving the network address of said respective ones of the devices (14) when the durations
exceeds a predetermined threshold value.

9. A method of operating a sub-network (12) that is coupled to a communication
network (10) via a firewall (23), the method comprising:
- statically assigning identifiers to devices (14) coupled to the sub-network (12)
and/or to services provided by said devices (14);
providing identifier based access policy rules for the devices and/or services;
- dynamically assigning network addresses to the devices;
- monitoring messages on the sub-network (12) to detect messages that associate the identifiers with network addresses assigned to devices (14) assigned to the identifiers;
- dynamically redefining firewall rules expressed in terms of the network addresses obtained by said monitoring, dependent on the access policy rules for the identifiers assigned to the devices and/or services for which the network addresses obtained by said monitoring are used.

10. A method according to claim 9, wherein the access policy rules include access policy rules for messages that have as destination address the network address used for a device (14) and/or service a specified identifier.

11. A method according to claim 10, wherein the firewall rules are initially defined to block all messages to devices (14) with network addresses within a range of network addresses that are available for dynamic assignment, said redefining including redefining rules to allow at least selected messages to pass through the firewall when these messages have a destination address to a particular one of the devices (14).

12. A method according to claim 10, wherein the access policy rules include access policy rules for messages that have a source address with a specified value or a value within a specified range.

13. A method according to claim 10, comprising forming a virtual private network, comprising a network tunnel between said network and a further sub-network, and applying the redefined firewall rules to messages received via said tunnel.

14. A method according to claim 13, comprising applying the redefined firewall rules only to messages received via said tunnel.

15. A method according to claim 11, comprising forming a plurality of virtual private networks, each comprising a network tunnel to a respective further sub-network (12), wherein the firewall policy rules differentiate between different ones of the further sub-
networks (12), said redefining including redefine firewall rules to allow at least selected messages from a first part of the further sub-networks (12) but not from a second part of the further sub-networks (12) to pass through the firewall when these messages have a destination address to a particular one of the devices (14) in the sub-network (12).

16. A method according to claim 9, comprising further monitoring messages on the sub-network (12) to detect a sign-off message from a particular one of the devices (14) and undoing redefinitions of the firewall rules for involving the network address of said particular one of the devices (14) in response to detection of the sign-off message.

17. A method according to claim 9, comprising maintaining time-out information, representative of durations of time intervals elapsed since respective ones of the devices (14) were last heard of on the sub-network and undoing redefinitions of the firewall rules for involving the network address of said respective ones of the devices (14) when the durations exceeds a predetermined threshold value.

18. A method according to claim 9, wherein said monitoring comprises selecting service advertisement messages, each of which defines a network address for a service, from among messages transmitted via the sub-network and deriving associations between the identifiers and network addresses form the advertisement messages.

19. A method according to claim 9, comprising transmitting, via the sub-network, search messages for devices and/or services assigned to respective identifiers, said monitoring comprising monitoring response messages to the search messages.

20. A method according to claim 9, wherein the identifiers are Universal Unique Identifiers.