

Claims of '474 Patent
[1.0] A method of filtering packets at a packet security gateway configured for protection of a network, wherein the packet security gateway is capable of receiving a plurality of dynamic security policies and is associated with a security policy management server external from the network, the method comprising:
[1.1] receiving, by the packet security gateway and from the security policy management server, a dynamic security policy comprising packet filtering rules,
[1.2] wherein one or both of the dynamic security policy or one or more of the packet filtering rules of the dynamic security policy were automatically created or altered, by the security policy management server, based on malicious traffic information received from a plurality of malicious host tracker services,
[1.3] wherein at least two of the plurality of malicious host tracker services are managed by different organizations,
[1.4] wherein one or more of the packet filtering rules were added, removed, or altered by the security policy management server based on a correlation between portions of the malicious traffic information, and
[1.5] wherein a first packet matching rule of the packet filtering rules comprises: at least one packet matching criterion, a corresponding packet transformation function, and an indication of a feed managed by at least one of the plurality of malicious host tracker services; and
[1.6] performing, based on the packet filtering rules, packet filtering on individual packets of a plurality of packets associated with the network protected by the packet security gateway,
[1.7] wherein the packet filtering comprises: inspecting individual packets; and
[1.8] filtering each packet based on content determined from the inspection of that individual packet.
[2.0] The method of claim 1, wherein the at least one packet matching criterion comprises at least one network address associated with an indication of malicious network traffic.

Claims of '474 Patent
[3.0] The method of claim 1, wherein at least one packet transformation function comprises a network protection action.
[4.0] The method of claim 1, wherein the dynamic security policy specifies that a first plurality of packets should be placed in a first forwarding queue and a second plurality of packets should be placed in a second forwarding queue,
[4.1] wherein the first forwarding queue has a higher forwarding rate than the second forwarding queue, and
[4.2] wherein the method further comprises: sending, by the packet security gateway, the first plurality of packets in the first forwarding queue; and sending, by the packet security gateway, the second plurality of packets in the second forwarding queue.
[5.0] The method of claim 1, further comprising: receiving, by the packet security gateway and using an interface that is not addressed at the network layer, packets in a network layer transparent manner; and
[5.1] performing at least one packet transformation function at the network layer.
[6.0] The method of claim 1, wherein the packet security gateway is a LAN switch.
[7.0] The method of claim 1, wherein the filtering each packet comprises: filtering one packet at a time; and
[7.1] performing a packet digest logging function with respect to each filtered packet.
[8.0] The method of claim 7, wherein, the packet digest logging function comprises: identifying a subset of information in each packet that is also specified by the packet digest logging function;
[8.1] generating, for each packet, a record comprising the subset of information;
[8.2] reformatting, for each packet, the subset of information according to a logging system standard; and

Claims of '474 Patent
[8.3] routing, based on the subset of information in the identified packet, each packet to a monitoring device.
[9.0] A packet security gateway configured for protection of a network, capable of receiving a plurality of dynamic security policies and associated with a security policy management server external from the network, the packet security gateway comprising:
[9.1] at least one processor; and
[9.2] memory comprising instructions that, when executed by the last least one processor, cause the packet security gateway to:
[9.3] receive, from the security policy management server, a dynamic security policy comprising packet filtering rules,
[9.4] wherein one or both of the dynamic security policy or one or more of the packet filtering rules of the dynamic security policy were automatically created or altered, by the security policy management server, based on malicious traffic information received from a plurality of malicious host tracker services,
[9.5] wherein at least two of the plurality of malicious host tracker services are managed by different organizations,
[9.6] wherein one or more of the packet filtering rules were added, removed, or altered by the security policy management server based on a correlation between portions of the malicious traffic information, and
[9.7] wherein a first packet matching rule of the packet filtering rules comprises: at least one packet matching criterion, a corresponding packet transformation function, and an indication of a feed managed by at least one of the plurality of malicious host tracker services; and
[9.8] perform, based on the packet filtering rules, packet filtering on individual packets of a plurality of packets associated with the network protected by the packet security gateway,
[9.9] wherein the packet filtering comprises: inspecting individual packets; and

Claims of '474 Patent
[9.10] filtering each packet based on content determined from the inspection of that individual packet.
[10.0] The packet security gateway of claim 9, wherein the at least one packet matching criterion comprises at least one network address associated with an indication of malicious network traffic.
[11.0] The packet security gateway of claim 9, wherein at least one packet transformation function comprises a network protection action.
[12.0] The packet security gateway of claim 9, wherein the dynamic security policy specifies that a first plurality of packets should be placed in a first forwarding queue and a second plurality of packets should be placed in a second forwarding queue,
[12.1] wherein the first forwarding queue has a higher forwarding rate than the second forwarding queue, and
[12.2] wherein the instructions, when executed by the at least one processor, cause the packet security gateway to: send the first plurality of packets in the first forwarding queue; and send the second plurality of packets in the second forwarding queue.
[13.0] The packet security gateway of claim 9, wherein the instructions, when executed by the at least one processor, cause the packet security gateway to: receive, using an interface that is not addressed at the network layer, packets in a network layer transparent manner; and
[13.1] perform at least one packet transformation function at the network layer.
[14.0] The packet security gateway of claim 9, wherein the packet security gateway is a LAN switch.
[15.0] The packet security gateway of claim 9, wherein the instructions, when executed by the at least one processor, cause the packet security gateway to: filter one packet at a time; and

Claims of '474 Patent
[15.1] perform a packet digest logging function with respect to each filtered packet.
[16.0] The packet security gateway of claim 15, wherein the packet digest logging function comprises: identifying a subset of information in each packet that is also specified by the packet digest logging function;
[16.1] generating, for each packet, a record comprising the subset of information;
[16.2] reformatting, for each packet, the subset of information according to a logging system standard; and
[16.3] routing, based on the subset of information in the identified packet, each packet to a monitoring device.
[17.0] One or more non-transitory computer-readable media comprising instructions that, when executed by one or more processors of a packet security gateway configured to protect a network, cause the packet security gateway to:
[17.1] receive, from a security policy management server, a dynamic security policy comprising packet filtering rules,
[17.2] wherein one or both of the dynamic security policy or one or more of the packet filtering rules of the dynamic security policy were automatically created or altered, by the security policy management server, based on malicious traffic information received from a plurality of malicious host tracker services,
[17.3] wherein at least two of the plurality of malicious host tracker services are managed by different organizations,
[17.4] wherein one or more of the packet filtering rules were added, removed, or altered by the security policy management server based on a correlation between portions of the malicious traffic information, and
[17.5] wherein a first packet matching rule of the packet filtering rules comprises: at least one packet matching criterion, a corresponding packet transformation function, and an indication of a feed managed by at least one of the plurality of malicious host tracker services; and

Claims of '474 Patent
[17.6] perform, based on the packet filtering rules, packet filtering on individual packets of a plurality of packets associated with the network protected by the packet security gateway,
[17.7] wherein the packet filtering comprises: inspecting individual packets; and
[17.8] filtering each packet based on content determined from the inspection of that individual packet.
[18.0] The one or more non-transitory computer-readable media of claim 17, wherein the at least one packet matching criterion comprises at least one network address associated with an indication of malicious network traffic.
[19.0] The one or more non-transitory computer-readable media of claim 17, wherein at least one packet transformation function comprises a network protection action.
[20.0] The one or more non-transitory computer-readable media of claim 17, wherein the dynamic security policy specifies that a first plurality of packets should be placed in a first forwarding queue and a second plurality of packets should be placed in a second forwarding queue,
[20.1] wherein the first forwarding queue has a higher forwarding rate than the second forwarding queue, and
[20.2] wherein the instructions, when executed by the one or more processors of the packet security gateway, cause the packet security gateway to: send the first plurality of packets in the first forwarding queue; and send the second plurality of packets in the second forwarding queue.
[21.0] The one or more non-transitory computer-readable media of claim 17, wherein the instructions, when executed by the one or more processors of the packet security gateway, cause the packet security gateway to: receive, using an interface that is not addressed at the network layer, packets in a network layer transparent manner; and
[21.1] perform at least one packet transformation function at the network layer.

Claims of '474 Patent
[22.0] The one or more non-transitory computer-readable media of claim 17, wherein the packet security gateway is a LAN switch.
[23.1] The one or more non-transitory computer-readable media of claim 17, wherein the instructions, when executed by the one or more processors of the packet security gateway, cause the packet security gateway to: filter one packet at a time; and
[23.2] perform a packet digest logging function with respect to each filtered packet.
[24.0] The one or more non-transitory computer-readable media of claim 23, wherein the packet digest logging function comprises: identifying a subset of information in the packet that is also specified by the packet digest logging function;
[24.1] generating, for each packet, a record comprising the subset of information;
[24.2] reformatting, for each packet, the subset of information according to a logging system standard; and
[24.3] routing, based on the subset of information in the identified packet, each packet to a monitoring device.
[25.0] A system comprising:
[25.1] a security policy management server external from a network associated with a packet security gateway, wherein the security policy management server comprises:
[25.2] one or more first processors; and
[25.3] first memory storing first instructions that, when executed by one or more first processors, cause the security policy management server to:
[25.4] receive, from a plurality of malicious host tracker services, first malicious traffic information, wherein at least two of the plurality of malicious host tracker services are managed by different organizations;

Claims of '474 Patent
[25.5] automatically create, based on the first malicious traffic information, a dynamic security policy or packet filtering rules of the dynamic security policy,
[25.6] wherein a first packet filtering rule of the packet filtering rules comprise: one or more packet matching criteria comprising a corresponding network addresses, one or more corresponding packet transformation functions, and an indication of a feed managed by at least one of the plurality of malicious host tracker services; and
[25.7] add, remove, or alter the one or more rules of the dynamic security policy based, at least in part, on making a correlation between portions of the first malicious traffic information;
[25.8] the packet security gateway, wherein the packet security gateway is configured for protection of a network and associated with the security policy management server external from the network, the packet security gateway comprising:
[25.9] one or more second processors; and
[25.10] second memory storing second instructions that, when executed by one or more second processors, cause the packet security gateway to:
[25.11] receive, from the security policy management server, the dynamic security policy comprising the packet filtering rules; and
[25.12] perform, based on the packet filtering rules, packet filtering on individual packets of a plurality of packets associated with the network protected by the packet security gateway, wherein the packet filtering comprises:
[25.13] inspecting individual packets; and
[25.14] filtering each packet based on content determined from the inspection of that individual packet.
[26.0] The system of claim 25, wherein the at least one packet matching criterion comprises at least one network address associated with an indication of malicious network traffic.

Claims of '474 Patent
[27.0] The system of claim 25, wherein at least one packet transformation function comprises a network protection action.
[28.0] The system of claim 25, wherein the dynamic security policy specifies that a first plurality of packets should be placed in a first forwarding queue and a second plurality of packets should be placed in a second forwarding queue,
[28.1] wherein the first forwarding queue has a higher forwarding rate than the second forwarding queue, and
[28.2] wherein the second instructions, when executed by the one or more second processors, further cause the packet security gateway to: send the first plurality of packets in the first forwarding queue; and send the second plurality of packets in the second forwarding queue.
[29.0] The system of claim 25, wherein the second instructions, when executed by the one or more second processors, further cause the packet security gateway to:
[29.1] receive, using an interface that is not addressed at the network layer, packets in a network layer transparent manner; and
[29.2] performing at least one packet transformation function at the network layer.
[30.0] The system of claim 25, wherein the packet security gateway is a LAN switch.
[31.0] The system of claim 25, wherein the second instructions, when executed by the one or more second processors, cause the packet security gateway to: filter one packet at a time; and
[31.1] perform a packet digest logging function with respect to each filtered packet.
[32.0] The system of claim 31, wherein, the packet digest logging function comprises: identifying a subset of information in each packet that is also specified by the packet digest logging function;

Claims of '474 Patent
[32.1] generating, for each packet, a record comprising the subset of information;
[32.2] reformatting, for each packet, the subset of information according to a logging system standard; and
[32.3] routing, based on the subset of information in the identified packet, each packet to a monitoring device.
[33.0] The system of claim 25, wherein at least one packet transformation function is configured to route associated packets to a monitoring device.