

## **'266 PATENT CLAIM LISTING**

| <b>'266 Patent – Claim 1</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>[1.0]</b>                 | A method of filtering packets at a packet security gateway, of a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected by the packet security gateway and one or more networks other than the network protected by the packet security gateway, the method comprising:                                                                                                                                                                                                                                                                                                                     |
| <b>[1.1]</b>                 | receiving, by the packet security gateway and from a security policy management server external from the network protected by the packet security gateway, a dynamic security policy comprising a first set of packet filtering rules to be applied to all network traffic traversing the boundary, wherein:                                                                                                                                                                                                                                                                                                                                                      |
| <b>[1.2]</b>                 | each packet filtering rule of the first set of packet filtering rules comprises at least one packet matching criterion and a corresponding packet transformation function, and                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>[1.3]</b>                 | one or more first packet filtering rules of the first set of packet filtering rules comprise packet matching criteria corresponding to one or more network addresses and were automatically created or altered by the security policy management server based on aggregated malicious traffic information received from at least one third party malicious host tracker service located in the one or more networks other than the network protected by the packet security gateway, that comprises network addresses that have been determined, by the at least one third party malicious host tracker service, to be associated with malicious network traffic; |
| <b>[1.4]</b>                 | performing, on a packet by packet basis, packet filtering on a first portion of packets corresponding to network traffic traversing the boundary via the packet security gateway based on the first set of packet filtering rules by performing at least one packet transformation function specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets;                                                                                                                                                                                                                                           |

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>[1.5]</b> | receiving, by the packet security gateway and after performing packet filtering on the first portion of the packets, an updated second set of packet filtering rules for the dynamic security policy from the security policy management server, wherein the updated second set of packet filtering rules comprises an update to the one or more first packet filtering rules created or altered by the security policy management server based on updated malicious traffic information received from the at least one third party malicious host tracker service; and |
| <b>[1.6]</b> | performing, on a packet by packet basis, packet filtering on a second portion of the packets corresponding to network traffic traversing the boundary via the packet security gateway based on the updated second set of packet filtering rules by performing at least one packet transformation function specified by at least one packet filtering rule of the second set of packet filtering rules on the second portion of packets.                                                                                                                                 |

#### **'266 Patent – Claim 2**

|              |                                                                                                                                                                                                                                                                                |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>[2.0]</b> | The method of claim 1, wherein the at least one packet matching criterion corresponding to the one or more first packet filtering rules automatically created or altered by the security policy management server comprises at least one of the one or more network addresses. |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### **'266 Patent – Claim 3**

|              |                                                                                                                                                                                                    |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>[3.0]</b> | The method of claim 1, wherein the at least one third party malicious host tracker service comprises a subscription service that aggregates information associated with malicious network traffic. |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### **'266 Patent – Claim 4**

|              |                                                                                                                                              |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>[4.0]</b> | The method of claim 1, wherein the one or more network addresses were associated, by a subscription service, with malicious network traffic. |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------|

#### **'266 Patent – Claim 5**

|              |                                                                                                                   |
|--------------|-------------------------------------------------------------------------------------------------------------------|
| <b>[5.0]</b> | The method of claim 1, wherein at least one packet transformation function comprises a network protective action. |
|--------------|-------------------------------------------------------------------------------------------------------------------|

| <b>'266 Patent – Claim 6</b> |                                                                                                                                                                                                             |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>[6.0]</b>                 | The method of claim 1, further comprising:                                                                                                                                                                  |
| <b>[6.1]</b>                 | receiving, by the packet security gateway, packets in a network layer transparent manner using an interface that is not addressed at the network layer; and                                                 |
| <b>[6.2]</b>                 | performing the at least one packet transformation function specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets at the network layer. |

| <b>'266 Patent – Claim 7</b> |                                                                                                                                                                                                                    |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>[7.0]</b>                 | The method of claim 1, wherein one or more packet filtering rules of the first set of packet filtering rules specify a packet transformation function other than forwarding or dropping the corresponding packets. |

| <b>'266 Patent – Claim 8</b> |                                                                                                                                                                                                                                                                                                   |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>[8.0]</b>                 | A packet security gateway, of a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected by the packet security gateway and one or more networks other than the network protected by the packet security gateway, comprising: |
| <b>[8.1]</b>                 | one or more processors; and                                                                                                                                                                                                                                                                       |
| <b>[8.2]</b>                 | memory storing instructions that, when executed by the one or more processors, cause the packet security gateway to:                                                                                                                                                                              |
| <b>[8.3]</b>                 | receive, from a security policy management server external from the network protected by the packet security gateway, a dynamic security policy comprising a first set of packet filtering rules to be applied to all network traffic traversing the boundary, wherein:                           |

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>[8.4]</b> | each packet filtering rule of the first set of packet filtering rules comprises at least one packet matching criterion and a corresponding packet transformation function, and                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>[8.5]</b> | one or more first packet filtering rules of the first set of packet filtering rules comprise packet matching criteria corresponding to one or more network addresses and were automatically created or altered by the security policy management server based on aggregated malicious traffic information, received from at least one third party malicious host tracker service located in the one or more networks other than the network protected by the packet security gateway, that comprises network addresses that have been determined, by the at least one third party malicious host tracker service, to be associated with malicious network traffic; |
| <b>[8.6]</b> | perform, on a packet by packet basis, packet filtering on a first portion of packets corresponding to network traffic traversing the boundary via the packet security gateway based on the first set of packet filtering rules by performing at least one packet transformation function specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets;                                                                                                                                                                                                                                               |
| <b>[8.7]</b> | receive, after performing packet filtering on the first portion of the packets, an updated second set of packet filtering rules for the dynamic security policy from the security policy management server, wherein the updated second set of packet filtering rules comprises an update to the one or more first packet filtering rules created or altered by the security policy management server based on updated malicious traffic information received from the at least one third party malicious host tracker service; and                                                                                                                                 |
| <b>[8.8]</b> | perform, on a packet by packet basis, packet filtering on a second portion of the packets corresponding to network traffic traversing the boundary via the packet security gateway based on the updated second set of packet filtering rules by performing at least one packet transformation function specified by at least one packet filtering rule of the second set of packet filtering rules on the second portion of packets.                                                                                                                                                                                                                               |

**'266 Patent – Claim 9**

|              |                                                                                                                                                                                                                                                                                                 |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>[9.0]</b> | The packet security gateway of claim 8, wherein the at least one packet matching criterion corresponding to the one or more first packet filtering rules automatically created or altered by the security policy management server comprises at least one of the one or more network addresses. |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

| <b>'266 Patent – Claim 10</b> |                                                                                                                                                                                                                     |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>[10.0]</b>                 | The packet security gateway of claim 8, wherein the at least one third party malicious host tracker service comprises a subscription service that aggregates information associated with malicious network traffic. |

| <b>'266 Patent – Claim 11</b> |                                                                                                                                                               |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>[11.0]</b>                 | The packet security gateway of claim 8, wherein the one or more network addresses were associated, by a subscription service, with malicious network traffic. |

| <b>'266 Patent – Claim 12</b> |                                                                                                                                    |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| <b>[12.0]</b>                 | The packet security gateway of claim 8, wherein at least one packet transformation function comprises a network protective action. |

| <b>'266 Patent – Claim 13</b> |                                                                                                                                                                                                          |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>[13.0]</b>                 | The packet security gateway of claim 8,                                                                                                                                                                  |
| <b>[13.1]</b>                 | wherein the instructions further cause the packet security gateway to: receive packets in a network layer transparent manner using an interface that is not addressed at the network layer; and          |
| <b>[13.2]</b>                 | perform the at least one packet transformation function specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets at the network layer. |

| <b>'266 Patent – Claim 14</b> |                                                                                                                                                                                                                                     |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>[14.0]</b>                 | The packet security gateway of claim 8, wherein one or more packet filtering rules of the first set of packet filtering rules specify a packet transformation function other than forwarding or dropping the corresponding packets. |

| <b>'266 Patent – Claim 15</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>[15.0]</b>                 | One or more non-transitory computer readable media storing instructions that, when executed by at least one processor, cause a packet security gateway, of a plurality of packet security gateways that collectively provide an entire interface across a boundary of a network protected by the packet security gateway and one or more networks other than the network protected by the packet security gateway, to perform steps comprising:                                                                                                                                                                                                                   |
| <b>[15.1]</b>                 | receiving, from a security policy management server external from the network protected by the packet security gateway, a dynamic security policy comprising a first set of packet filtering rules to be applied to all network traffic traversing the boundary, wherein:                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>[15.2]</b>                 | each packet filtering rule of the first set of packet filtering rules comprises at least one packet matching criterion and a corresponding packet transformation function, and                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>[15.3]</b>                 | one or more first packet filtering rules of the first set of packet filtering rules comprise packet matching criteria corresponding to one or more network addresses and were automatically created or altered by the security policy management server based on aggregated malicious traffic information received from at least one third party malicious host tracker service located in the one or more networks other than the network protected by the packet security gateway, that comprises network addresses that have been determined, by the at least one third party malicious host tracker service, to be associated with malicious network traffic; |

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>[15.4]</b> | performing, on a packet by packet basis, packet filtering on a first portion of packets corresponding to network traffic traversing the boundary via the packet security gateway based on the first set of packet filtering rules by performing at least one packet transformation function specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets;                                                                                                              |
| <b>[15.5]</b> | receiving, after performing packet filtering on the first portion of the packets, an updated second set of packet filtering rules for the dynamic security policy from the security policy management server, wherein the updated second set of packet filtering rules comprises an update to the one or more first packet filtering rules created or altered by the security policy management server based on updated malicious traffic information received from the at least one third party malicious host tracker service; and |
| <b>[15.6]</b> | performing, on a packet by packet basis, packet filtering on a second portion of the packets corresponding to network traffic traversing the boundary via the packet security gateway based on the updated second set of packet filtering rules by performing at least one packet transformation function specified by at least one packet filtering rule of the second set of packet filtering rules on the second portion of packets.                                                                                              |

#### **'266 Patent – Claim 16**

|               |                                                                                                                                                                                                                                                                                                  |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>[16.0]</b> | The computer readable media of claim 15, wherein the at least one packet matching criterion corresponding to the one or more first packet filtering rules automatically created or altered by the security policy management server comprises at least one of the one or more network addresses. |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### **'266 Patent – Claim 17**

|               |                                                                                                                                                                                                                                                                                                                                                |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>[17.0]</b> | The computer readable media of claim 15, wherein the at least one third party malicious host tracker service comprises a subscription service that aggregates information associated with malicious network traffic, and wherein the one or more network addresses were associated, by a subscription service, with malicious network traffic. |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

| <b>'266 Patent – Claim 18</b> |                                                                                                                                     |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| <b>[18.0]</b>                 | The computer readable media of claim 15, wherein at least one packet transformation function comprises a network protective action. |

| <b>'266 Patent – Claim 19</b> |                                                                                                                                                                                                             |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>[19.0]</b>                 | The computer readable media of claim 15, further comprising:                                                                                                                                                |
| <b>[19.1]</b>                 | receiving, by the packet security gateway, packets in a network layer transparent manner using an interface that is not addressed at the network layer; and                                                 |
| <b>[19.2]</b>                 | performing the at least one packet transformation function specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets at the network layer. |

| <b>'266 Patent – Claim 20</b> |                                                                                                                                                                                                                                      |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>[20.0]</b>                 | The computer readable media of claim 15, wherein one or more packet filtering rules of the first set of packet filtering rules specify a packet transformation function other than forwarding or dropping the corresponding packets. |

| <b>'266 Patent – Claim 21</b> |                                                                                                                                                                                                             |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>[21.0]</b>                 | A method of filtering packets at a packet security gateway configured for protection of a network and associated with a security policy management server external from the network, the method comprising: |
| <b>[21.1]</b>                 | receiving, by the packet security gateway, a dynamic security policy comprising a first set of packet filtering rules from the security policy management server,                                           |
| <b>[21.2]</b>                 | wherein each packet filtering rule of the first set of packet filtering rules comprises at least one packet matching criterion and a corresponding packet transformation function, and                      |

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>[21.3]</b> | wherein one or more first packet filtering rules of the first set of packet filtering rules comprise packet matching criteria corresponding to one or more network addresses and were automatically created or altered by the security policy management server based on aggregated malicious traffic information received from at least one third party malicious host tracker service located in the one or more networks other than the network protected by the packet security gateway, that comprises network addresses that have been determined, by the at least one third party malicious host tracker service, to be associated with malicious network traffic; |
| <b>[21.4]</b> | performing, on a packet by packet basis, packet filtering on a first portion of packets associated with the network protected by the packet security gateway based on the first set of packet filtering rules by performing at least one of multiple packet transformation functions specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets;                                                                                                                                                                                                                                                          |
| <b>[21.5]</b> | receiving, by the packet security gateway and after performing packet filtering on the first portion of the packets, an updated second set of packet filtering rules for the dynamic security policy from the security policy management server, wherein the updated second set of packet filtering rules comprises an update to the one or more first packet filtering rules created or altered by the security policy management server based on updated malicious traffic information received from the at least one third party malicious host tracker service; and                                                                                                   |
| <b>[21.6]</b> | performing, on a packet by packet basis, packet filtering on a second portion of the packets associated with the network protected by the packet security gateway based on the updated second set of packet filtering rules.                                                                                                                                                                                                                                                                                                                                                                                                                                              |

| <b>'266 Patent – Claim 22</b> |                                                                                                                                                                                                                                                                                 |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>[22.0]</b>                 | The method of claim 21, wherein the at least one packet matching criterion corresponding to the one or more first packet filtering rules automatically created or altered by the security policy management server comprises at least one of the one or more network addresses. |

| <b>'266 Patent – Claim 23</b> |                                                                                                                                                                                                     |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>[23.0]</b>                 | The method of claim 21, wherein the at least one third party malicious host tracker service comprises a subscription service that aggregates information associated with malicious network traffic. |

| <b>'266 Patent – Claim 24</b> |                                                                                                                                               |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>[24.0]</b>                 | The method of claim 21, wherein the one or more network addresses were associated, by a subscription service, with malicious network traffic. |

| <b>'266 Patent – Claim 25</b> |                                                                                                                    |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>[25.0]</b>                 | The method of claim 21, wherein at least one packet transformation function comprises a network protective action. |

| <b>'266 Patent – Claim 26</b> |                                                                                                                                                                                                             |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>[26.0]</b>                 | The method of claim 21, further comprising:                                                                                                                                                                 |
| <b>[26.1]</b>                 | receiving, by the packet security gateway, packets in a network layer transparent manner using an interface that is not addressed at the network layer; and                                                 |
| <b>[26.2]</b>                 | performing the at least one packet transformation function specified by at least one packet filtering rule of the first set of packet filtering rules on the first portion of packets at the network layer. |

| <b>'266 Patent – Claim 27</b> |                                                                                                                                                                                                                     |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>[27.0]</b>                 | The method of claim 21, wherein one or more packet filtering rules of the first set of packet filtering rules specify a packet transformation function other than forwarding or dropping the corresponding packets. |