

Ex. G-2 - Invalidity of U.S. Patent No. 8,397,282 against U.S. 6,154,775 to Coss et al. ("Coss")

Fortinet, Inc. ("Fortinet") provides this chart subject to all reservations, objections, statements, and disclaimers set forth herein and in Fortinet's Preliminary Invalidity Contentions Cover Pleading, as well as any amendment, supplement, or modification thereof, which are incorporated herein by reference in their entirety.

On information and belief, and subject to further investigation and discovery, Coss issued November 28, 2000, and is thus available as prior art under at least pre-AIA §102(b).

As illustrated in the chart below, Coss anticipates the asserted claims of the '710 Patent. To the extent Coss is found not to expressly disclose certain limitations in the asserted claims, such limitations are inherent. To the extent Coss is found not to anticipate any asserted claims or claim elements of the '710 Patent, the reference nevertheless renders those claims or claim elements obvious under 35 U.S.C. § 103, either alone or in combination with other art identified in the cover pleading or herein. These Preliminary Invalidity Contentions are not an admission by Fortinet that the accused products, including any current or past versions of the accused products, are covered by, or infringe the asserted claims, but are based instead on the recognition that if the claims are interpreted to be broad enough to encompass the accused products, the claims must also be construed to have that same scope when considering whether they are invalid.

The following chart is partially based on, but is not limited by, the claim constructions implicit in Plaintiff's Infringement Contentions, to the extent that such constructions are apparent from the Infringement Contentions. Fortinet notes that in many instances, Plaintiff's Infringement Contentions fail to provide adequate notice of Plaintiff's construction of the asserted claims and fail to comply with the Court's scheduling order and other applicable rules. Fortinet does not accept the assumptions concerning the scope and meaning implicit in Plaintiff's Infringement Contentions, to the extent those assumptions are discernible, and reserves the right to challenge Plaintiff's proposed (or implied) constructions. Fortinet also reserves the right to revise and supplement these charts if and when Plaintiff is permitted to provide revised Infringement Contentions or otherwise make its positions known. To the extent that these Preliminary Invalidity Contentions rely on or otherwise embody particular constructions of terms or phrases in the asserted claims, Fortinet does not necessarily advocate any such construction as proper constructions of those terms or phrase. Fortinet also reserves the right to revise and supplement these charts after the Court construes the claims. Citations given in the chart below are merely representative of the respective elements and are not meant to be exhaustive.

Claim	Exemplary Citation from Coss
<p>[1PRE] A method for controlling data through a firewall performed on at least one data controlling computer having computer instructions stored on at least one non-transitory computer readable medium, comprising:</p>	<p>Coss discloses and/or renders obvious a method for controlling data through a firewall performed on at least one data controlling computer having computer instructions stored on at least one non-transitory computer readable medium.</p> <p><i>E.g.:</i></p> <p>Claim 35: "A method for providing a firewall service in a computer network, comprising the steps of: forming an augmented set of rules by including, in an already-loaded initial set of access rules, at least one dynamic rule which acts to alter the operation of the already-loaded initial set of rules under specified conditions without reloading at least one unaltered rule of the already-loaded set of access rules; and using the augmented set of rules in validating a packet; wherein the at least one rule is a dynamic rule and further wherein the dynamic rule has associated therewith at least one set of data which is pointed to by the dynamic rule, such that the data within the set can be changed to alter the operation of the rule without changing the rule itself."</p> <p>Coss at Abstract: "The invention provides improved computer network firewalls which include one or more features for increased processing efficiency. A firewall in accordance with the invention can support multiple security policies, multiple users or both, by applying any one of several distinct sets of access rules. The firewall can also be configured to utilize "stateful" packet filtering which involves caching rule processing results for one or more packets, and then utilizing the cached results to bypass rule processing for subsequent similar packets. To facilitate passage to a user, by a firewall, of a separate later transmission which is properly in response to an original transmission, a dependency mask can be set based on session data items such as source host address, destination host address, and type of service. The mask can be used to query a cache of active sessions being processed by the firewall, such that a rule can be selected based on the number of sessions that satisfy the query. Dynamic rules may be used in addition to pre-loaded access rules in order to simplify rule processing. To unburden the firewall of application proxies, the firewall can be enabled to redirect a network session to a separate server for processing."</p>

Claim	Exemplary Citation from Coss
	<p>Coss at 1:9-11: "This invention relates to the prevention of unauthorized access in computer networks and, more particularly, to firewall protection within computer networks."</p> <p>Coss at 1:14-26: "In computer networks, information is conventionally transmitted in the form of packets. Information present at one site may be accessed by or transmitted to another site at the command of the former or the latter. Thus, e.g., if information is proprietary, there is a need for safeguards against unauthorized access. To this end, techniques known as packet filtering, effected at a network processor component known as a firewall, have been developed and commercialized. At the firewall, packets are inspected and filtered, i.e., passed on or dropped depending on whether they conform to a set of predefined access rules. Conventionally, these rule sets are represented in tabular form."</p> <p>Coss at 2:33-46: "In accordance with a fourth aspect of the invention, a computer network firewall may make use of dynamic rules which are added to a set of access rules for processing packets. The dynamic rules allow a given rule set to be modified based on events happening in the network without requiring that the entire rule set be reloaded. Exemplary dynamic rules include a "one-time" rule which is only used for a single session, a time-limited rule which is used only for a specified time period, and a threshold rule which is used only when certain conditions are satisfied. Other types of dynamic rules include rules which define a host group, such that the host group can be modified to add or drop different hosts without altering other aspects of the access rule set."</p> <p>Coss at 3:25-35: "The preferred techniques can be implemented at a firewall for controlling the flow of data between, for example, separate local area networks (LANs) or subnets of a LAN. Exemplary embodiments of the invention are described herein in terms of processes. Efficient prototypes of such processes have been implemented as computer system software, using the "C" programming language for implementation on general-purpose PC hardware. Efficiency can be enhanced further, as is known, by special-purpose firmware or hardware computer system implementations."</p>

Claim	Exemplary Citation from Coss
	<p>Coss at 3:36-4:3:</p> <p>"1. Support for Multiple Security Domains With a capability for supporting multiple security domains, a single firewall can support multiple users, each with a separate security policy. Also, as different security policies can apply for communications between sub-sites, such a capability can be used within a site. Respective configurations are illustrated by FIGS. 1 and 2. FIG. 1 shows four user sites 101-104, e.g., of corporations A through D, with firewall protection in their connections to the Internet 105. Such protection is provided by a firewall facility, here in the form of a LAN 110, including firewall processors 111, 113 and 114, an administrator processor 115, a router 116 and a web server 117. Each of firewall processors 113 and 114 is dedicated to a single site, namely respective sites 103 and 104. Firewall processor 111 is configured to serve the two sites 101 and 102. Firewall processor 111 implements separate firewall policies for each of the two sites vis-a-vis the Internet 105, as well as for communications between the two sites. A process for preferred operation of the firewall processor 111 is described below with reference to FIGS. 5A and 5B, including properly selecting among different firewall policies. FIG. 2 shows a user site 201 connected to the Internet 105 via a firewall processor 211. An administrator processor 215 and a router 216 are connected to the firewall processor 211. The router 216 is connected to additional firewall processors 212 and 213 which are internal to the user site 201. The firewall processor 212 protects a single sub-site 223, such as Human Resources (HR). The firewall processor 213 is configured for protecting two sub-sites, such as Payroll (P) and Disbursements (D), vis-a-vis the remainder of the site 201 as well as with respect to communications between sub-sites 221 and 222. This can be achieved by employing the process illustrated by FIGS. 5A and 5B in the firewall processor 213."</p> <p>Coss at 8:28-40:</p> <p>"Dynamic rules are rules which are included with the access rules as a need arises, for processing along with the access rules, e.g., by a rule processing engine. Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions. A dynamic rule can be set for single-session use, or its use can be limited as to time. Once a dynamic rule has served its function, it can be</p>

Claim	Exemplary Citation from Coss
	<p>removed from the rule set. The dynamic rules allow a given rule set to be modified based on events happening in the network without requiring that the entire rule set be reloaded."</p>
<p>[1A] defining at least one node, wherein the at least one node is associated with two or more network interfaces;</p>	<p>Coss discloses and/or renders obvious defining at least one node, wherein the at least one node is associated with two or more network interfaces.</p> <p><i>E.g.:</i></p> <p>Coss at 1:61-2:6: "The present invention provides techniques for implementing computer network firewalls so as to improve processing efficiency, improve security, increase access rule flexibility, and enhance the ability of a firewall to deal with complex protocols. In accordance with a first aspect of the invention, a computer network firewall is able to support (a) multiple security policies, (b) multiple users, or (c) multiple security policies as well as multiple users, by applying any one of several distinct sets of access rules for a given packet. The particular rule set that is applied for any packet can be determined based on information such as the incoming and outgoing network interfaces as well as the network source and destination addresses."</p> <p>Coss at 3:25-35: "The preferred techniques can be implemented at a firewall for controlling the flow of data between, for example, separate local area networks (LANs) or subnets of a LAN. Exemplary embodiments of the invention are described herein in terms of processes. Efficient prototypes of such processes have been implemented as computer system software, using the "C" programming language for implementation on general-purpose PC hardware. Efficiency can be enhanced further, as is known, by special-purpose firmware or hardware computer system implementations."</p> <p>Coss at 3:36-4:3: "1. Support for Multiple Security Domains With a capability for supporting multiple security domains, a single firewall can support multiple users, each with a separate security policy. Also, as different security policies can apply for communications between sub-sites, such a capability can be used within a site. Respective configurations are illustrated by FIGS. 1 and 2.</p>

Claim	Exemplary Citation from Coss
	<p>FIG. 1 shows four user sites 101-104, e.g., of corporations A through D, with firewall protection in their connections to the Internet 105. Such protection is provided by a firewall facility, here in the form of a LAN 110, including firewall processors 111, 113 and 114, an administrator processor 115, a router 116 and a web server 117. Each of firewall processors 113 and 114 is dedicated to a single site, namely respective sites 103 and 104. Firewall processor 111 is configured to serve the two sites 101 and 102. Firewall processor 111 implements separate firewall policies for each of the two sites vis-a-vis the Internet 105, as well as for communications between the two sites. A process for preferred operation of the firewall processor 111 is described below with reference to FIGS. 5A and 5B, including properly selecting among different firewall policies.</p> <p>FIG. 2 shows a user site 201 connected to the Internet 105 via a firewall processor 211. An administrator processor 215 and a router 216 are connected to the firewall processor 211. The router 216 is connected to additional firewall processors 212 and 213 which are internal to the user site 201. The firewall processor 212 protects a single sub-site 223, such as Human Resources (HR). The firewall processor 213 is configured for protecting two sub-sites, such as Payroll (P) and Disbursements (D), vis-a-vis the remainder of the site 201 as well as with respect to communications between sub-sites 221 and 222. This can be achieved by employing the process illustrated by FIGS. 5A and 5B in the firewall processor 213."</p> <p>Coss at 6:18-28: "FIGS. 5A and 5B illustrate over-all flow for packet processing by a firewall which supports multiple domains. Such processing includes determining the domains which the packet is to cross, examining the applicable rules to ascertain whether the packet may pass, and determining whether any special processing is required. In the firewall, each domain is associated with one or more network interfaces. Interfaces that support more than one domain are separated using an IP address range to distinguish the packets. The following steps are included:"</p> <p>Coss at 6:33-37: "503: on the basis of which interface received the packet and the source IP address of the received packet, the source domain is determined as described separately below with reference to FIGS. 6 and 7; if no domain is found, the process skips to step 505;"</p>

Claim	Exemplary Citation from Coss															
	<p data-bbox="596 235 808 261">Coss at 7:10-15:</p> <p data-bbox="596 272 1898 375">"For convenient linking of each network interface to a domain, a domain table is used. In cases where an interface is shared by multiple domains, an address range is included. This is illustrated by FIG. 6 which shows non-overlapping address ranges."</p> <p data-bbox="596 418 705 444">Figure 6</p> <div data-bbox="1018 516 1486 537" style="text-align: center;"> <p>U.S. Patent Nov. 28, 2000 Sheet 7 of 12 6,154,775</p> </div> <table border="1" data-bbox="1041 721 1446 1019" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th data-bbox="1041 721 1136 792">INTERFACE</th> <th data-bbox="1136 721 1346 792">ADDRESS RANGE</th> <th data-bbox="1346 721 1446 792">DOMAIN</th> </tr> </thead> <tbody> <tr> <td data-bbox="1041 792 1136 857" style="text-align: center;">0</td> <td data-bbox="1136 792 1346 857" style="text-align: center;">10.50.0.0 - 10.50.255.255</td> <td data-bbox="1346 792 1446 857" style="text-align: center;">A</td> </tr> <tr> <td data-bbox="1041 857 1136 922" style="text-align: center;">0</td> <td data-bbox="1136 857 1346 922" style="text-align: center;">10.60.0.0 - 10.60.255.255</td> <td data-bbox="1346 857 1446 922" style="text-align: center;">B</td> </tr> <tr> <td data-bbox="1041 922 1136 987" style="text-align: center;">1</td> <td data-bbox="1136 922 1346 987" style="text-align: center;">*</td> <td data-bbox="1346 922 1446 987" style="text-align: center;">C</td> </tr> <tr> <td data-bbox="1041 987 1136 1019" style="text-align: center;">2</td> <td data-bbox="1136 987 1346 1019" style="text-align: center;">*</td> <td data-bbox="1346 987 1446 1019" style="text-align: center;">*</td> </tr> </tbody> </table> <p data-bbox="1213 1068 1283 1094" style="text-align: center;">FIG. 6</p>	INTERFACE	ADDRESS RANGE	DOMAIN	0	10.50.0.0 - 10.50.255.255	A	0	10.60.0.0 - 10.60.255.255	B	1	*	C	2	*	*
INTERFACE	ADDRESS RANGE	DOMAIN														
0	10.50.0.0 - 10.50.255.255	A														
0	10.60.0.0 - 10.60.255.255	B														
1	*	C														
2	*	*														

Claim	Exemplary Citation from Coss
<p>[1B] associating a set of firewall rules with the at least one node;</p>	<p>Coss discloses and/or renders obvious associating a set of firewall rules with the at least one node.</p> <p><i>E.g.:</i></p> <p>Coss at 1:61-2:6: "The present invention provides techniques for implementing computer network firewalls so as to improve processing efficiency, improve security, increase access rule flexibility, and enhance the ability of a firewall to deal with complex protocols. In accordance with a first aspect of the invention, a computer network firewall is able to support (a) multiple security policies, (b) multiple users, or (c) multiple security policies as well as multiple users, by applying any one of several distinct sets of access rules for a given packet. The particular rule set that is applied for any packet can be determined based on information such as the incoming and outgoing network interfaces as well as the network source and destination addresses."</p> <p>Coss at 2:33-46: "In accordance with a fourth aspect of the invention, a computer network firewall may make use of dynamic rules which are added to a set of access rules for processing packets. The dynamic rules allow a given rule set to be modified based on events happening in the network without requiring that the entire rule set be reloaded. Exemplary dynamic rules include a "one-time" rule which is only used for a single session, a time-limited rule which is used only for a specified time period, and a threshold rule which is used only when certain conditions are satisfied. Other types of dynamic rules include rules which define a host group, such that the host group can be modified to add or drop different hosts without altering other aspects of the access rule set."</p> <p>Coss at 3:36-4:3: "1. Support for Multiple Security Domains With a capability for supporting multiple security domains, a single firewall can support multiple users, each with a separate security policy. Also, as different security policies can apply for communications between sub-sites, such a capability can be used within a site. Respective configurations are illustrated by FIGS. 1 and 2. FIG. 1 shows four user sites 101-104, e.g., of corporations A through D, with firewall protection in their connections to the Internet 105. Such protection is provided by a firewall facility, here in the</p>

Claim	Exemplary Citation from Coss
	<p>form of a LAN 110, including firewall processors 111, 113 and 114, an administrator processor 115, a router 116 and a web server 117. Each of firewall processors 113 and 114 is dedicated to a single site, namely respective sites 103 and 104. Firewall processor 111 is configured to serve the two sites 101 and 102. Firewall processor 111 implements separate firewall policies for each of the two sites vis-a-vis the Internet 105, as well as for communications between the two sites. A process for preferred operation of the firewall processor 111 is described below with reference to FIGS. 5A and 5B, including properly selecting among different firewall policies.</p> <p>FIG. 2 shows a user site 201 connected to the Internet 105 via a firewall processor 211. An administrator processor 215 and a router 216 are connected to the firewall processor 211. The router 216 is connected to additional firewall processors 212 and 213 which are internal to the user site 201. The firewall processor 212 protects a single sub-site 223, such as Human Resources (HR). The firewall processor 213 is configured for protecting two sub-sites, such as Payroll (P) and Disbursements (D), vis-a-vis the remainder of the site 201 as well as with respect to communications between sub-sites 221 and 222. This can be achieved by employing the process illustrated by FIGS. 5A and 5B in the firewall processor 213."</p> <p>Coss at 4:4-19: "The security policies can be represented by sets of access rules which are represented in tabular form and which are loaded into the firewall by a firewall administrator. As illustrated in FIG. 3, such a table can provide for categories including rule number, designations of source and destination hosts, a designation of a special service which can be called for in a packet, and a specification of an action to be taken on a packet. Special services can include proxy services, network address translation, and encryption, for example. In FIG. 3, the categories "Source Host," "Destination Host" and "Service" impose conditions which must be satisfied by data included in a packet for the specified action to be taken on that packet. Other conditions can be included, and such conditions need not relate to data included in the packet. For example, application of a rule can be made conditional on the time of day or day of the week."</p> <p>Coss at 6:18-28: "FIGS. 5A and 5B illustrate over-all flow for packet processing by a firewall which supports multiple domains. Such processing includes determining the domains which the packet is to cross, examining the applicable rules to ascertain whether the packet may pass, and determining whether any special</p>

Claim	Exemplary Citation from Coss
	<p>processing is required. In the firewall, each domain is associated with one or more network interfaces. Interfaces that support more than one domain are separated using an IP address range to distinguish the packets. The following steps are included:"</p> <p>Coss at 6:29-30: "501: an IP packet is received by the firewall at an interface;"</p> <p>Coss at 6:33-65: "503: on the basis of which interface received the packet and the source IP address of the received packet, the source domain is determined as described separately below with reference to FIGS. 6 and 7; if no domain is found, the process skips to step 505; 504: using the session key from step 502, the cache of the source domain is searched for a match; if a match is found in the cache and if the action is not "drop," the process continues with step 505; if a match is found in the cache and the action is "drop," the packet is dropped and the process returns to step 501; if no match is found in the cache, the rule set for the source domain is searched for a match; if a match is found in the rules and if the action is not "drop," the process continues with step 505; if a match is found in the rules and the action is "drop," a corresponding entry is included in the cache, the packet is dropped, and the process returns to step 501; if no match is found in the rules, the packet is dropped and the process returns to step 501; 505: the destination interface is determined using the local area network (LAN) address of the packet, and, if the source domain rule specifies a destination interface, using that destination interface and a routing table; 506: using the destination interface and the destination address of the packet, the destination domain is determined; if the destination domain is not found, or if the destination domain matches the domain just checked, the process skips to step 508; 507: cache look-up and, if required, rule set look-up for the destination domain are carried out in a manner analogous to that employed for the source domain in step 504;"</p> <p>Coss at 7:10-15: "For convenient linking of each network interface to a domain, a domain table is used. In cases where an interface is shared by multiple domains, an address range is included. This is illustrated by FIG. 6 which shows non-overlapping address ranges."</p>

Claim	Exemplary Citation from Coss
<p>[1C] receiving a packet at a first node of the at least one node; and</p>	<p>Coss discloses and/or renders obvious receiving a packet at a first node of the at least one node.</p> <p><i>E.g.:</i></p> <p>Coss at 6:18-28: "FIGS. 5A and 5B illustrate over-all flow for packet processing by a firewall which supports multiple domains. Such processing includes determining the domains which the packet is to cross, examining the applicable rules to ascertain whether the packet may pass, and determining whether any special processing is required. In the firewall, each domain is associated with one or more network interfaces. Interfaces that support more than one domain are separated using an IP address range to distinguish the packets. The following steps are included:"</p> <p>Coss at 6:29-30: "501: an IP packet is received by the firewall at an interface;"</p> <p>Coss at 7:64-65: "901: the packet is obtained and the session key is extracted;"</p> <p>Coss at 9:33: "1001: packet is received by the firewall;"</p> <p>Coss at 9:52-53: "1006: the packet is received in the remote proxy server application;"</p>
<p>[1D] accepting or denying the packet based on the set of firewall rules, wherein the set of firewall rules is dynamically self-configurable during runtime without operator interaction,</p>	<p>Coss discloses and/or renders obvious accepting or denying the packet based on the set of firewall rules, wherein the set of firewall rules is dynamically self-configurable during runtime without operator interaction, wherein the set of firewall rules comprises a plurality of chains of rules forming various paths through a hierarchical structure, and wherein the hierarchical structure comprises defined places for dynamically updating the set of firewall rules during runtime.</p>

Claim	Exemplary Citation from Coss
<p>wherein the set of firewall rules comprises a plurality of chains of rules forming various paths through a hierarchical structure, and wherein the hierarchical structure comprises defined places for dynamically updating the set of firewall rules during runtime.</p>	<p><u>E.g.:</u></p> <p>Claim 35: "A method for providing a firewall service in a computer network, comprising the steps of: forming an augmented set of rules by including, in an already-loaded initial set of access rules, at least one dynamic rule which acts to alter the operation of the already-loaded initial set of rules under specified conditions without reloading at least one unaltered rule of the already-loaded set of access rules; and using the augmented set of rules in validating a packet; wherein the at least one rule is a dynamic rule and further wherein the dynamic rule has associated therewith at least one set of data which is pointed to by the dynamic rule, such that the data within the set can be changed to alter the operation of the rule without changing the rule itself."</p> <p>Coss at Abstract: "The invention provides improved computer network firewalls which include one or more features for increased processing efficiency. A firewall in accordance with the invention can support multiple security policies, multiple users or both, by applying any one of several distinct sets of access rules. The firewall can also be configured to utilize "stateful" packet filtering which involves caching rule processing results for one or more packets, and then utilizing the cached results to bypass rule processing for subsequent similar packets. To facilitate passage to a user, by a firewall, of a separate later transmission which is properly in response to an original transmission, a dependency mask can be set based on session data items such as source host address, destination host address, and type of service. The mask can be used to query a cache of active sessions being processed by the firewall, such that a rule can be selected based on the number of sessions that satisfy the query. Dynamic rules may be used in addition to pre-loaded access rules in order to simplify rule processing. To unburden the firewall of application proxies, the firewall can be enabled to redirect a network session to a separate server for processing."</p> <p>Coss at 1:61-2:6: "The present invention provides techniques for implementing computer network firewalls so as to improve processing efficiency, improve security, increase access rule flexibility, and enhance the ability of a firewall to deal with complex protocols. In accordance with a first aspect of the invention, a computer network firewall is able to support (a) multiple security policies, (b) multiple users, or (c)</p>

Claim	Exemplary Citation from Coss
	<p>multiple security policies as well as multiple users, by applying any one of several distinct sets of access rules for a given packet. The particular rule set that is applied for any packet can be determined based on information such as the incoming and outgoing network interfaces as well as the network source and destination addresses."</p> <p>Coss at 2:7-20: "In accordance with a second aspect of the invention, a computer network firewall can be configured to utilize "stateful" packet filtering which improves performance by storing the results of rule processing applied to one or more packets. Stateful packet filtering may be implemented by caching rule processing results for one or more packets, and then utilizing the cached results to bypass rule processing for subsequent similar packets. For example, the results of applying a rule set to a particular packet of a network session may be cached, such that when a subsequent packet from the same network session arrives in the firewall, the cached results from the previous packet are used for the subsequent packet. This avoids the need to apply the rule set to each incoming packet."</p> <p>Coss at 2:21-32: "In accordance with a third aspect of the invention, a computer network firewall authorizes or prevents certain network sessions using a dependency mask which can be set based on session data items such as source host address, destination host address, and type of service. The dependency mask can be used to query a cache of active sessions being processed by the firewall, to thereby identify the number of sessions that satisfy the query. The query may be associated with an access rule, such that the selection of that particular rule is dependent on the number of successful matches to the query."</p> <p>Coss at 2:33-46: "In accordance with a fourth aspect of the invention, a computer network firewall may make use of dynamic rules which are added to a set of access rules for processing packets. The dynamic rules allow a given rule set to be modified based on events happening in the network without requiring that the entire rule set be reloaded. Exemplary dynamic rules include a "one-time" rule which is only used for a single session, a time-limited rule which is used only for a specified time period, and a threshold rule which is used only when certain conditions are satisfied. Other types of dynamic rules</p>

Claim	Exemplary Citation from Coss
	<p>include rules which define a host group, such that the host group can be modified to add or drop different hosts without altering other aspects of the access rule set."</p> <p>Coss at 4:4-19: "The security policies can be represented by sets of access rules which are represented in tabular form and which are loaded into the firewall by a firewall administrator. As illustrated in FIG. 3, such a table can provide for categories including rule number, designations of source and destination hosts, a designation of a special service which can be called for in a packet, and a specification of an action to be taken on a packet. Special services can include proxy services, network address translation, and encryption, for example. In FIG. 3, the categories "Source Host," "Destination Host" and "Service" impose conditions which must be satisfied by data included in a packet for the specified action to be taken on that packet. Other conditions can be included, and such conditions need not relate to data included in the packet. For example, application of a rule can be made conditional on the time of day or day of the week."</p> <p>Coss at 4:21-26: "When a category provided for in the rule table is irrelevant in a certain rule, the corresponding table entry can be marked as a "wild card." This can apply to any one or any combination of the categories. In FIG. 3 and elsewhere, an asterisk (*) is used for wild card entries. "FTP" stands for "file transfer protocol.""</p> <p>Coss at 4:27-37: "In rule processing for a packet, the rules are applied sequentially until a rule is found which is satisfied by the packet (or until the rule table is exhausted, in which case the packet is dropped). For a packet to satisfy a rule, each condition included in the rule must be met. For example, with reference to FIG. 3, a packet from source host A to destination host D and representing mail will be dropped under Rule 20. The following is a more detailed list of exemplary rule set categories in accordance with the invention. The first five category names correspond to the categories shown in FIG. 3."</p> <p>Coss at 5:38-52: "A computer network firewall in accordance with the invention can be configured to utilize "stateful" packet filtering which improves performance by storing in a cache the results of rule processing as</p>

Claim	Exemplary Citation from Coss
	<p>applied to one or more packets. Stateful packet filtering may be implemented by caching rule processing results for received packets, and then utilizing the cached results to bypass rule processing for subsequent similar packets. For example, the results of applying a rule set to a packet of a given network session may be cached, such that when a subsequent packet from the same network session arrives in the firewall, the cached results from the previous packet are used for the subsequent packet. This avoids the need to apply the rule set to each incoming packet, and thereby provides substantial performance advantages over conventional firewalls."</p> <p>Coss at 6:18-28: "FIGS. 5A and 5B illustrate over-all flow for packet processing by a firewall which supports multiple domains. Such processing includes determining the domains which the packet is to cross, examining the applicable rules to ascertain whether the packet may pass, and determining whether any special processing is required. In the firewall, each domain is associated with one or more network interfaces. Interfaces that support more than one domain are separated using an IP address range to distinguish the packets. The following steps are included:"</p> <p>Coss at 6:29-30: "501: an IP packet is received by the firewall at an interface;"</p> <p>Coss at 6:31-32: "502: the session key is obtained from the IP header of the packet;"</p> <p>Coss at 6:33-7:9: "503: on the basis of which interface received the packet and the source IP address of the received packet, the source domain is determined as described separately below with reference to FIGS. 6 and 7; if no domain is found, the process skips to step 505; 504: using the session key from step 502, the cache of the source domain is searched for a match; if a match is found in the cache and if the action is not "drop," the process continues with step 505; if a match is found in the cache and the action is "drop," the packet is dropped and the process returns to step 501; if no match is found in the cache, the rule set for the source domain is searched for a match; if a match is found in the rules and if the action is not "drop," the process continues with step 505; if a match is found in the rules and the action is "drop," a corresponding entry is included in the cache,</p>

Claim	Exemplary Citation from Coss
	<p>the packet is dropped, and the process returns to step 501; if no match is found in the rules, the packet is dropped and the process returns to step 501;</p> <p>505: the destination interface is determined using the local area network (LAN) address of the packet, and, if the source domain rule specifies a destination interface, using that destination interface and a routing table;</p> <p>506: using the destination interface and the destination address of the packet, the destination domain is determined; if the destination domain is not found, or if the destination domain matches the domain just checked, the process skips to step 508;</p> <p>507: cache look-up and, if required, rule set look-up for the destination domain are carried out in a manner analogous to that employed for the source domain in step 504;</p> <p>508: if a rule that applies to the packet calls for an address change, e.g., to a proxy or for insertion of one packet into another ("tunnel option"), the process returns to step 505 for processing based on the changed destination;</p> <p>509: if the packet was not processed with respect to any domain, the packet can be dropped, as a firewall owner has no interest in supporting communications between interfaces which are not subject to any access rules;</p> <p>510: with all actions having resulted in "pass," the packet is sent out the appropriate network interface."</p> <p>Coss at 7:15-27: "FIG. 7 illustrates domain table processing as performed in steps 503 and 506 described above, including the following steps: 701: the domain table is searched for a match of the interface name; 702: if a matching table entry is found, and if the IP address range is present in the matching table entry, the packet address is checked as to whether it is within the range; if so, the specified domain is selected; otherwise, the search continues with the next table entry; 703: if the end of the table is reached without a match having been found, no action is taken."</p> <p>Coss at 8:27-59: "4. Dynamic Rules Dynamic rules are rules which are included with the access rules as a need arises, for processing along with the access rules, e.g., by a rule processing engine. Dynamic rules can include unique,</p>

Claim	Exemplary Citation from Coss
	<p>current information such as, for example, specific source and destination port numbers. They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions. A dynamic rule can be set for single-session use, or its use can be limited as to time. Once a dynamic rule has served its function, it can be removed from the rule set. The dynamic rules allow a given rule set to be modified based on events happening in the network without requiring that the entire rule set be reloaded.</p> <p>Exemplary dynamic rules include a "one-time" rule which is only used for a single session, a time-limited rule which is used only for a specified time period, and a threshold rule which is used only when certain conditions are satisfied. Another type of dynamic rule includes rules which define a host group, such that the host group can be modified to add or drop different hosts without altering other aspects of the access rule set. Other dynamic rules may be used to facilitate rule setup in certain specific types of processing applications. For example, an FTP proxy application could use a dynamic rule to authorize establishment of an FTP data channel in response to a data request. The dynamic rule in this example would typically not be loaded until a data request is made over the FTP control session, and could be limited to one use and made active for only a limited time period. The rule set therefore need not include a separate data channel rule for use with all requests. As a result, the rule specification and rule processing are simplified, and security is improved."</p> <p>Coss at 9:28-10:21: "In implementing proxy reflection, dynamic rules can be used as described below for an illustrative embodiment, with reference to FIGS. 10A and 10B. FIG. 10A illustrates proxy reflection processing including the following steps at the firewall: 1001: packet is received by the firewall; 1002: action associated with the packet is determined by looking in the appropriate session cache or, if not found in the cache, in the appropriate rule set; if the action is "pass" or "proxy," packet processing continues; if the action is "drop," the packet is dropped; 1003: if the action indicates a proxy application supported locally on the firewall, the packet is sent up the protocol stack to an awaiting proxy application; 1004: if the action indicates a remote proxy, the packet's destination address is replaced with the address of the remote proxy; if configured, the destination port can be changed as well; the original packet header data is recorded in the session cache along with any changed values; 1005: the packet is routed to the remote proxy server.</p>

Claim	Exemplary Citation from Coss
	<p>FIG. 10B illustrates processing at the remote proxy, subsequent to step 1005, including the following steps:</p> <p>1006: the packet is received in the remote proxy server application;</p> <p>1007: the remote proxy contacts the firewall for the original session key for the packet;</p> <p>1008: the remote proxy application uses the original session key to perform its function, such as dropping the connection based on its own security model, performing the requested service, or contacting the original destination address on behalf of the user; if the remote proxy is using single reflection, the process skips to step 1011;</p> <p>1009: the remote proxy application contacts the firewall over the encrypted channel to request dual reflection capability;</p> <p>1010: the firewall determines a new destination port number that will guarantee uniqueness of the connection from the server; the firewall passes this new port number and the original session key back to the proxy application;</p> <p>1011: the remote proxy application requests permission from the firewall for a connection from itself to the original destination;</p> <p>1012: the firewall loads a dynamic rule to perform this action;</p> <p>1013: the remote proxy sends the packet to the firewall; based on the dynamic rule loaded in step 1012, the firewall forwards the packet to the original destination; in the case of dual reflection, the proxy uses the destination port which was determined by the firewall in step 1010, and, as the packet passes through the firewall, the IP header values are changed back to the original values.</p> <p>All future packets associated with the same session are processed alike, except that steps 1007 and 1009-1012 can be skipped. This is because the same dynamic rules apply for the life of the session."</p>
<p>[2] A method according to claim 1, wherein dynamically updating the set of firewall rules during runtime further comprises, during runtime, adding a rule to the set of firewall rules, deleting a rule from the set of firewall rules, or</p>	<p>Coss discloses and/or renders obvious a method according to claim 1, wherein dynamically updating the set of firewall rules during runtime further comprises, during runtime, adding a rule to the set of firewall rules, deleting a rule from the set of firewall rules, or modifying a rule in the set of firewall rules without operator interaction.</p> <p><i>E.g.</i>:</p>

Claim	Exemplary Citation from Coss
<p>modifying a rule in the set of firewall rules without operator interaction.</p>	<p>Claim 35: "A method for providing a firewall service in a computer network, comprising the steps of: forming an augmented set of rules by including, in an already-loaded initial set of access rules, at least one dynamic rule which acts to alter the operation of the already-loaded initial set of rules under specified conditions without reloading at least one unaltered rule of the already-loaded set of access rules; and using the augmented set of rules in validating a packet; wherein the at least one rule is a dynamic rule and further wherein the dynamic rule has associated therewith at least one set of data which is pointed to by the dynamic rule, such that the data within the set can be changed to alter the operation of the rule without changing the rule itself."</p> <p>Coss at 2:33-46: "In accordance with a fourth aspect of the invention, a computer network firewall may make use of dynamic rules which are added to a set of access rules for processing packets. The dynamic rules allow a given rule set to be modified based on events happening in the network without requiring that the entire rule set be reloaded. Exemplary dynamic rules include a "one-time" rule which is only used for a single session, a time-limited rule which is used only for a specified time period, and a threshold rule which is used only when certain conditions are satisfied. Other types of dynamic rules include rules which define a host group, such that the host group can be modified to add or drop different hosts without altering other aspects of the access rule set."</p> <p>Coss at 8:28-40: "Dynamic rules are rules which are included with the access rules as a need arises, for processing along with the access rules, e.g., by a rule processing engine. Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions. A dynamic rule can be set for single-session use, or its use can be limited as to time. Once a dynamic rule has served its function, it can be removed from the rule set. The dynamic rules allow a given rule set to be modified based on events happening in the network without requiring that the entire rule set be reloaded."</p>

Claim	Exemplary Citation from Coss
	<p>Coss at 8:41-59: "Exemplary dynamic rules include a "one-time" rule which is only used for a single session, a time-limited rule which is used only for a specified time period, and a threshold rule which is used only when certain conditions are satisfied. Another type of dynamic rule includes rules which define a host group, such that the host group can be modified to add or drop different hosts without altering other aspects of the access rule set. Other dynamic rules may be used to facilitate rule setup in certain specific types of processing applications. For example, an FTP proxy application could use a dynamic rule to authorize establishment of an FTP data channel in response to a data request. The dynamic rule in this example would typically not be loaded until a data request is made over the FTP control session, and could be limited to one use and made active for only a limited time period. The rule set therefore need not include a separate data channel rule for use with all requests. As a result, the rule specification and rule processing are simplified, and security is improved."</p> <p>Coss at 10:7-9: "1012: the firewall loads a dynamic rule to perform this action;"</p>
<p>[3] A method according to claim 1, wherein associating the set of firewall rules with the at least one node further comprises associating a first subset of the set of firewall rules with the first node.</p>	<p>Coss discloses and/or renders obvious a method according to claim 1, wherein associating the set of firewall rules with the at least one node further comprises associating a first subset of the set of firewall rules with the first node.</p> <p><i>E.g.:</i></p> <p>Coss at 3:37-42: "With a capability for supporting multiple security domains, a single firewall can support multiple users, each with a separate security policy. Also, as different security policies can apply for communications between sub-sites, such a capability can be used within a site. Respective configurations are illustrated by FIGS. 1 and 2."</p> <p>Coss at 3:43-57: "FIG. 1 shows four user sites 101-104, e.g., of corporations A through D, with firewall protection in their connections to the Internet 105. Such protection is provided by a firewall facility, here in the form of a LAN 110, including firewall processors 111, 113 and 114, an administrator processor 115, a router 116 and a web server 117. Each of firewall processors 113 and 114 is dedicated to a single site,</p>

Claim	Exemplary Citation from Coss
	<p>namely respective sites 103 and 104. Firewall processor 111 is configured to serve the two sites 101 and 102. Firewall processor 111 implements separate firewall policies for each of the two sites vis-a-vis the Internet 105, as well as for communications between the two sites. A process for preferred operation of the firewall processor 111 is described below with reference to FIGS. 5A and 5B, including properly selecting among different firewall policies."</p> <p>Coss at 3:58-4:3: "FIG. 2 shows a user site 201 connected to the Internet 105 via a firewall processor 211. An administrator processor 215 and a router 216 are connected to the firewall processor 211. The router 216 is connected to additional firewall processors 212 and 213 which are internal to the user site 201. The firewall processor 212 protects a single sub-site 223, such as Human Resources (HR). The firewall processor 213 is configured for protecting two sub-sites, such as Payroll (P) and Disbursements (D), vis-a-vis the remainder of the site 201 as well as with respect to communications between sub-sites 221 and 222. This can be achieved by employing the process illustrated by FIGS. 5A and 5B in the firewall processor 213."</p> <p>Coss at 4:4-19: "The security policies can be represented by sets of access rules which are represented in tabular form and which are loaded into the firewall by a firewall administrator. As illustrated in FIG. 3, such a table can provide for categories including rule number, designations of source and destination hosts, a designation of a special service which can be called for in a packet, and a specification of an action to be taken on a packet. Special services can include proxy services, network address translation, and encryption, for example. In FIG. 3, the categories "Source Host," "Destination Host" and "Service" impose conditions which must be satisfied by data included in a packet for the specified action to be taken on that packet. Other conditions can be included, and such conditions need not relate to data included in the packet. For example, application of a rule can be made conditional on the time of day or day of the week."</p> <p>Coss at 6:62-65: "507: cache look-up and, if required, rule set look-up for the destination domain are carried out in a manner analogous to that employed for the source domain in step 504;"</p>

Claim

Exemplary Citation from Coss

Figure 1

U.S. Patent Nov. 28, 2000 Sheet 1 of 12 6,154,775

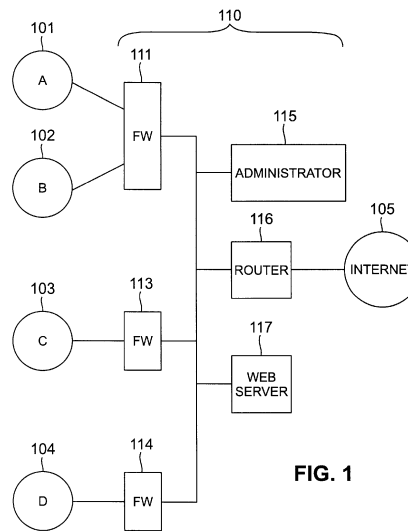
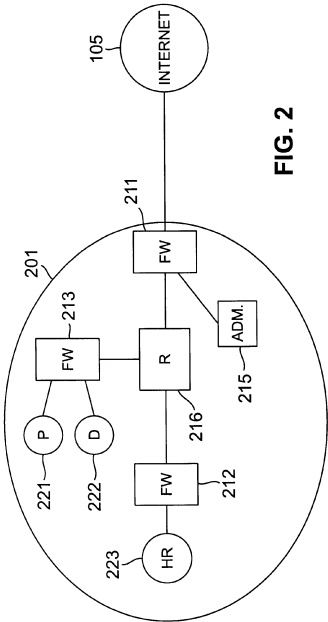


FIG. 1

Claim	Exemplary Citation from Coss
	<p data-bbox="594 237 705 264">Figure 2</p> <div data-bbox="1018 337 1486 358" style="text-align: center;"> <p>U.S. Patent Nov. 28, 2000 Sheet 2 of 12 6,154,775</p> </div>  <p data-bbox="1360 505 1388 578" style="text-align: center;">FIG. 2</p>
<p data-bbox="201 1195 573 1398">[4] A method according to claim 3, wherein the at least one node further comprises at least two nodes including a second node, further comprising associating a</p>	<p data-bbox="594 1195 1871 1295">Coss discloses and/or renders obvious a method according to claim 3, wherein the at least one node further comprises at least two nodes including a second node, further comprising associating a second subset of the set of firewall rules with the second node.</p> <p data-bbox="594 1341 667 1369"><u>E.g.</u>:</p>

Claim	Exemplary Citation from Coss
<p>second subset of the set of firewall rules with the second node.</p>	<p>Coss at 3:37-42: "With a capability for supporting multiple security domains, a single firewall can support multiple users, each with a separate security policy. Also, as different security policies can apply for communications between sub-sites, such a capability can be used within a site. Respective configurations are illustrated by FIGS. 1 and 2."</p> <p>Coss at 3:43-57: "FIG. 1 shows four user sites 101-104, e.g., of corporations A through D, with firewall protection in their connections to the Internet 105. Such protection is provided by a firewall facility, here in the form of a LAN 110, including firewall processors 111, 113 and 114, an administrator processor 115, a router 116 and a web server 117. Each of firewall processors 113 and 114 is dedicated to a single site, namely respective sites 103 and 104. Firewall processor 111 is configured to serve the two sites 101 and 102. Firewall processor 111 implements separate firewall policies for each of the two sites vis-a-vis the Internet 105, as well as for communications between the two sites. A process for preferred operation of the firewall processor 111 is described below with reference to FIGS. 5A and 5B, including properly selecting among different firewall policies."</p> <p>Coss at 3:58-4:3: "FIG. 2 shows a user site 201 connected to the Internet 105 via a firewall processor 211. An administrator processor 215 and a router 216 are connected to the firewall processor 211. The router 216 is connected to additional firewall processors 212 and 213 which are internal to the user site 201. The firewall processor 212 protects a single sub-site 223, such as Human Resources (HR). The firewall processor 213 is configured for protecting two sub-sites, such as Payroll (P) and Disbursements (D), vis-a-vis the remainder of the site 201 as well as with respect to communications between sub-sites 221 and 222. This can be achieved by employing the process illustrated by FIGS. 5A and 5B in the firewall processor 213."</p> <p>Coss at 7:10-15: "For convenient linking of each network interface to a domain, a domain table is used. In cases where an interface is shared by multiple domains, an address range is included. This is illustrated by FIG. 6 which shows non-overlapping address ranges."</p>

Claim

Exemplary Citation from Coss

Figure 1

U.S. Patent Nov. 28, 2000 Sheet 1 of 12 6,154,775

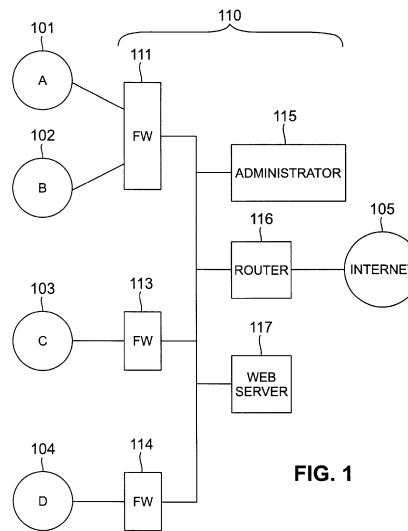


FIG. 1

Claim

Exemplary Citation from Coss

Figure 2

U.S. Patent Nov. 28, 2000 Sheet 2 of 12 6,154,775

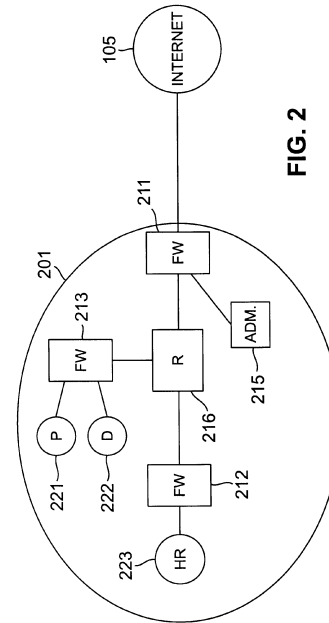


FIG. 2

Claim	Exemplary Citation from Coss															
	<p data-bbox="594 237 709 264">Figure 6</p> <p data-bbox="1020 342 1482 358">U.S. Patent Nov. 28, 2000 Sheet 7 of 12 6,154,775</p> <table border="1" data-bbox="1041 545 1446 846"> <thead> <tr> <th data-bbox="1041 545 1136 618">INTERFACE</th> <th data-bbox="1136 545 1346 618">ADDRESS RANGE</th> <th data-bbox="1346 545 1446 618">DOMAIN</th> </tr> </thead> <tbody> <tr> <td data-bbox="1041 618 1136 675">0</td> <td data-bbox="1136 618 1346 675">10.50.0.0 - 10.50.255.255</td> <td data-bbox="1346 618 1446 675">A</td> </tr> <tr> <td data-bbox="1041 675 1136 732">0</td> <td data-bbox="1136 675 1346 732">10.60.0.0 - 10.60.255.255</td> <td data-bbox="1346 675 1446 732">B</td> </tr> <tr> <td data-bbox="1041 732 1136 789">1</td> <td data-bbox="1136 732 1346 789">*</td> <td data-bbox="1346 732 1446 789">C</td> </tr> <tr> <td data-bbox="1041 789 1136 846">2</td> <td data-bbox="1136 789 1346 846">*</td> <td data-bbox="1346 789 1446 846">*</td> </tr> </tbody> </table> <p data-bbox="1213 894 1283 911">FIG. 6</p>	INTERFACE	ADDRESS RANGE	DOMAIN	0	10.50.0.0 - 10.50.255.255	A	0	10.60.0.0 - 10.60.255.255	B	1	*	C	2	*	*
INTERFACE	ADDRESS RANGE	DOMAIN														
0	10.50.0.0 - 10.50.255.255	A														
0	10.60.0.0 - 10.60.255.255	B														
1	*	C														
2	*	*														
<p data-bbox="201 1195 552 1365">[5] A method according to claim 4, wherein the first subset of firewall rules is the same as or at least partially different from the</p>	<p data-bbox="594 1195 1833 1260">Coss discloses and/or renders obvious a method according to claim 4, wherein the first subset of firewall rules is the same as or at least partially different from the second subset of firewall rules.</p> <p data-bbox="594 1300 667 1333"><u>E.g.:</u></p> <p data-bbox="594 1373 814 1398">Coss at Abstract:</p>															

Claim	Exemplary Citation from Coss
<p>second subset of firewall rules.</p>	<p>"The invention provides improved computer network firewalls which include one or more features for increased processing efficiency. A firewall in accordance with the invention can support multiple security policies, multiple users or both, by applying any one of several distinct sets of access rules. The firewall can also be configured to utilize "stateful" packet filtering which involves caching rule processing results for one or more packets, and then utilizing the cached results to bypass rule processing for subsequent similar packets. To facilitate passage to a user, by a firewall, of a separate later transmission which is properly in response to an original transmission, a dependency mask can be set based on session data items such as source host address, destination host address, and type of service. The mask can be used to query a cache of active sessions being processed by the firewall, such that a rule can be selected based on the number of sessions that satisfy the query. Dynamic rules may be used in addition to pre-loaded access rules in order to simplify rule processing. To unburden the firewall of application proxies, the firewall can be enabled to redirect a network session to a separate server for processing."</p> <p>Coss at 1:61-2:6: "The present invention provides techniques for implementing computer network firewalls so as to improve processing efficiency, improve security, increase access rule flexibility, and enhance the ability of a firewall to deal with complex protocols. In accordance with a first aspect of the invention, a computer network firewall is able to support (a) multiple security policies, (b) multiple users, or (c) multiple security policies as well as multiple users, by applying any one of several distinct sets of access rules for a given packet. The particular rule set that is applied for any packet can be determined based on information such as the incoming and outgoing network interfaces as well as the network source and destination addresses."</p> <p>Coss at 6:3-17: "In the firewall, a decision module or engine, here called a "domain support engine" (DSE) determines which security policy to use for a new network session. Each new session must be approved by the security policies of the source domain and the destination domain(s). For connections going to the Internet, it is likely that only a single domain check is performed. The DSE makes the domain selection based on the incoming or outgoing network interface, as well as on the source or destination network address of each packet. Inclusion, in packets, of source or destination addresses allows for multiple users to be supported by a single network interface. The incoming or</p>

Claim	Exemplary Citation from Coss
	<p>outgoing network interface may be in the form of a network interface card (NIC), e.g., an Intel EtherExpress Pro 100B card available from Intel Corporation."</p> <p>Coss at 6:62-65: "507: cache look-up and, if required, rule set look-up for the destination domain are carried out in a manner analogous to that employed for the source domain in step 504;"</p>
<p>[6] A method according to claim 4, wherein one of the first subset of firewall rules or second subset of firewall rules equals the entire set of firewall rules.</p>	<p>Coss discloses and/or renders obvious a method according to claim 4, wherein one of the first subset of firewall rules or second subset of firewall rules equals the entire set of firewall rules.</p> <p><u>E.g.:</u></p> <p>Coss at Abstract: "The invention provides improved computer network firewalls which include one or more features for increased processing efficiency. A firewall in accordance with the invention can support multiple security policies, multiple users or both, by applying any one of several distinct sets of access rules. The firewall can also be configured to utilize "stateful" packet filtering which involves caching rule processing results for one or more packets, and then utilizing the cached results to bypass rule processing for subsequent similar packets. To facilitate passage to a user, by a firewall, of a separate later transmission which is properly in response to an original transmission, a dependency mask can be set based on session data items such as source host address, destination host address, and type of service. The mask can be used to query a cache of active sessions being processed by the firewall, such that a rule can be selected based on the number of sessions that satisfy the query. Dynamic rules may be used in addition to pre-loaded access rules in order to simplify rule processing. To unburden the firewall of application proxies, the firewall can be enabled to redirect a network session to a separate server for processing."</p> <p>Coss at 1:61-2:6: "The present invention provides techniques for implementing computer network firewalls so as to improve processing efficiency, improve security, increase access rule flexibility, and enhance the ability of a firewall to deal with complex protocols. In accordance with a first aspect of the invention, a computer network firewall is able to support (a) multiple security policies, (b) multiple users, or (c)</p>

Claim	Exemplary Citation from Coss
	<p>multiple security policies as well as multiple users, by applying any one of several distinct sets of access rules for a given packet. The particular rule set that is applied for any packet can be determined based on information such as the incoming and outgoing network interfaces as well as the network source and destination addresses."</p> <p>Coss at 2:33-46: "In accordance with a fourth aspect of the invention, a computer network firewall may make use of dynamic rules which are added to a set of access rules for processing packets. The dynamic rules allow a given rule set to be modified based on events happening in the network without requiring that the entire rule set be reloaded. Exemplary dynamic rules include a "one-time" rule which is only used for a single session, a time-limited rule which is used only for a specified time period, and a threshold rule which is used only when certain conditions are satisfied. Other types of dynamic rules include rules which define a host group, such that the host group can be modified to add or drop different hosts without altering other aspects of the access rule set."</p>
<p>[7] A method according to claim 1, further comprising, after receiving the packet and prior to accepting or denying the packet, conditioning the packet based on the set of firewall rules.</p>	<p>Coss discloses and/or renders obvious a method according to claim 1, further comprising, after receiving the packet and prior to accepting or denying the packet, conditioning the packet based on the set of firewall rules.</p> <p><i>E.g.:</i></p> <p>Coss at 4:4-19: "The security policies can be represented by sets of access rules which are represented in tabular form and which are loaded into the firewall by a firewall administrator. As illustrated in FIG. 3, such a table can provide for categories including rule number, designations of source and destination hosts, a designation of a special service which can be called for in a packet, and a specification of an action to be taken on a packet. Special services can include proxy services, network address translation, and encryption, for example. In FIG. 3, the categories "Source Host," "Destination Host" and "Service" impose conditions which must be satisfied by data included in a packet for the specified action to be taken on that packet. Other conditions can be included, and such conditions need not relate to data included in the packet. For example, application of a rule can be made conditional on the time of day or day of the week."</p>

Claim	Exemplary Citation from Coss
	<p>Coss at 6:66-7:3: "508: if a rule that applies to the packet calls for an address change, e.g., to a proxy or for insertion of one packet into another ("tunnel option"), the process returns to step 505 for processing based on the changed destination;"</p> <p>Coss at 9:42-48: "1004: if the action indicates a remote proxy, the packet's destination address is replaced with the address of the remote proxy; if configured, the destination port can be changed as well; the original packet header data is recorded in the session cache along with any changed values;"</p>
<p>[8] A method according to claim 7, wherein conditioning the packet based on the set of firewall rules further comprises rewriting a portion of a network packet header associated with the packet.</p>	<p>Coss discloses and/or renders obvious a method according to claim 7, wherein conditioning the packet based on the set of firewall rules further comprises rewriting a portion of a network packet header associated with the packet.</p> <p><u>E.g.:</u></p> <p>Coss at 6:66-7:3: "508: if a rule that applies to the packet calls for an address change, e.g., to a proxy or for insertion of one packet into another ("tunnel option"), the process returns to step 505 for processing based on the changed destination;"</p> <p>Coss at 8:61-9:9: "Proxy reflection in accordance with the present invention involves redirecting a network session to another, "remote" proxy server for processing, and then later passing it back via the firewall to the intended destination. When a new session enters the firewall, a decision is made to determine whether service by a proxy server is required. If so, the firewall replaces the destination address in the packet with the host address of the proxy application and, if necessary, it can also change the service port. When the proxy application receives the session, it will request from the firewall the original destination address of the session for determining whether the connection to the destination is authorized. If the proxy then makes the connection to that destination as itself, using its own IP address, the service provided by the firewall will be called "single reflection" or "one-way reflection.""</p>

Claim	Exemplary Citation from Coss
	<p>Coss at 9:42-48: "1004: if the action indicates a remote proxy, the packet's destination address is replaced with the address of the remote proxy; if configured, the destination port can be changed as well; the original packet header data is recorded in the session cache along with any changed values;"</p> <p>Coss at 10:10-17: "1013: the remote proxy sends the packet to the firewall; based on the dynamic rule loaded in step 1012, the firewall forwards the packet to the original destination; in the case of dual reflection, the proxy uses the destination port which was determined by the firewall in step 1010, and, as the packet passes through the firewall, the IP header values are changed back to the original values."</p>
<p>[9] A method according to claim 1, wherein each of the at least one node is associated with at least two network interfaces.</p>	<p>Coss discloses and/or renders obvious a method according to claim 1, wherein each of the at least one node is associated with at least two network interfaces.</p> <p><i>E.g.:</i></p> <p>Coss at 1:61-2:6: "The present invention provides techniques for implementing computer network firewalls so as to improve processing efficiency, improve security, increase access rule flexibility, and enhance the ability of a firewall to deal with complex protocols. In accordance with a first aspect of the invention, a computer network firewall is able to support (a) multiple security policies, (b) multiple users, or (c) multiple security policies as well as multiple users, by applying any one of several distinct sets of access rules for a given packet. The particular rule set that is applied for any packet can be determined based on information such as the incoming and outgoing network interfaces as well as the network source and destination addresses."</p> <p>Coss at 6:3-17: "In the firewall, a decision module or engine, here called a "domain support engine" (DSE) determines which security policy to use for a new network session. Each new session must be approved by the security policies of the source domain and the destination domain(s). For connections going to the Internet, it is likely that only a single domain check is performed. The DSE makes the domain selection based on the incoming or outgoing network interface, as well as on the</p>

Claim	Exemplary Citation from Coss
	<p>source or destination network address of each packet. Inclusion, in packets, of source or destination addresses allows for multiple users to be supported by a single network interface. The incoming or outgoing network interface may be in the form of a network interface card (NIC), e.g., an Intel EtherExpress Pro 100B card available from Intel Corporation."</p> <p>Coss at 6:18-28: "FIGS. 5A and 5B illustrate over-all flow for packet processing by a firewall which supports multiple domains. Such processing includes determining the domains which the packet is to cross, examining the applicable rules to ascertain whether the packet may pass, and determining whether any special processing is required. In the firewall, each domain is associated with one or more network interfaces. Interfaces that support more than one domain are separated using an IP address range to distinguish the packets. The following steps are included:"</p>
<p>[10] A method according to claim 1, wherein each of the two or more network interfaces is connected with at least one physical device.</p>	<p>Coss discloses and/or renders obvious a method according to claim 1, wherein each of the two or more network interfaces is connected with at least one physical device.</p> <p><u>E.g.:</u></p> <p>Coss at 3:43-57: "FIG. 1 shows four user sites 101-104, e.g., of corporations A through D, with firewall protection in their connections to the Internet 105. Such protection is provided by a firewall facility, here in the form of a LAN 110, including firewall processors 111, 113 and 114, an administrator processor 115, a router 116 and a web server 117. Each of firewall processors 113 and 114 is dedicated to a single site, namely respective sites 103 and 104. Firewall processor 111 is configured to serve the two sites 101 and 102. Firewall processor 111 implements separate firewall policies for each of the two sites vis-a-vis the Internet 105, as well as for communications between the two sites. A process for preferred operation of the firewall processor 111 is described below with reference to FIGS. 5A and 5B, including properly selecting among different firewall policies."</p> <p>Coss at 3:58-4:3: "FIG. 2 shows a user site 201 connected to the Internet 105 via a firewall processor 211. An administrator processor 215 and a router 216 are connected to the firewall processor 211. The router</p>

Claim	Exemplary Citation from Coss
	<p>216 is connected to additional firewall processors 212 and 213 which are internal to the user site 201. The firewall processor 212 protects a single sub-site 223, such as Human Resources (HR). The firewall processor 213 is configured for protecting two sub-sites, such as Payroll (P) and Disbursements (D), vis-a-vis the remainder of the site 201 as well as with respect to communications between sub-sites 221 and 222. This can be achieved by employing the process illustrated by FIGS. 5A and 5B in the firewall processor 213."</p> <p>Coss at 6:3-17: "In the firewall, a decision module or engine, here called a "domain support engine" (DSE) determines which security policy to use for a new network session. Each new session must be approved by the security policies of the source domain and the destination domain(s). For connections going to the Internet, it is likely that only a single domain check is performed. The DSE makes the domain selection based on the incoming or outgoing network interface, as well as on the source or destination network address of each packet. Inclusion, in packets, of source or destination addresses allows for multiple users to be supported by a single network interface. The incoming or outgoing network interface may be in the form of a network interface card (NIC), e.g., an Intel EtherExpress Pro 100B card available from Intel Corporation."</p> <p>Coss at 6:18-28: "FIGS. 5A and 5B illustrate over-all flow for packet processing by a firewall which supports multiple domains. Such processing includes determining the domains which the packet is to cross, examining the applicable rules to ascertain whether the packet may pass, and determining whether any special processing is required. In the firewall, each domain is associated with one or more network interfaces. Interfaces that support more than one domain are separated using an IP address range to distinguish the packets. The following steps are included:"</p>
<p>[11] A method according to claim 1, wherein the set of firewall rules being dynamically self-configurable further comprises dynamically</p>	<p>Coss discloses and/or renders obvious method according to claim 1, wherein the set of firewall rules being dynamically self-configurable further comprises dynamically updating the set of firewall rules during runtime without operator interaction.</p> <p><u>E.g.:</u></p>

Claim	Exemplary Citation from Coss
<p>updating the set of firewall rules during runtime without operator interaction.</p>	<p>Claim 35: "A method for providing a firewall service in a computer network, comprising the steps of: forming an augmented set of rules by including, in an already-loaded initial set of access rules, at least one dynamic rule which acts to alter the operation of the already-loaded initial set of rules under specified conditions without reloading at least one unaltered rule of the already-loaded set of access rules; and using the augmented set of rules in validating a packet; wherein the at least one rule is a dynamic rule and further wherein the dynamic rule has associated therewith at least one set of data which is pointed to by the dynamic rule, such that the data within the set can be changed to alter the operation of the rule without changing the rule itself."</p> <p>Coss at 2:33-46: "In accordance with a fourth aspect of the invention, a computer network firewall may make use of dynamic rules which are added to a set of access rules for processing packets. The dynamic rules allow a given rule set to be modified based on events happening in the network without requiring that the entire rule set be reloaded. Exemplary dynamic rules include a "one-time" rule which is only used for a single session, a time-limited rule which is used only for a specified time period, and a threshold rule which is used only when certain conditions are satisfied. Other types of dynamic rules include rules which define a host group, such that the host group can be modified to add or drop different hosts without altering other aspects of the access rule set."</p> <p>Coss at 8:28-40: "Dynamic rules are rules which are included with the access rules as a need arises, for processing along with the access rules, e.g., by a rule processing engine. Dynamic rules can include unique, current information such as, for example, specific source and destination port numbers. They can be loaded at any time by trusted parties, e.g., a trusted application, remote proxy or firewall administrator, to authorize specific network sessions. A dynamic rule can be set for single-session use, or its use can be limited as to time. Once a dynamic rule has served its function, it can be removed from the rule set. The dynamic rules allow a given rule set to be modified based on events happening in the network without requiring that the entire rule set be reloaded."</p>

Claim	Exemplary Citation from Coss
	<p>Coss at 9:66-10:3: "1010: the firewall determines a new destination port number that will guarantee uniqueness of the connection from the server; the firewall passes this new port number and the original session key back to the proxy application;"</p> <p>Coss at 10:4-6: "1011: the remote proxy application requests permission from the firewall for a connection from itself to the original destination;"</p> <p>Coss at 10:7-9: "1012: the firewall loads a dynamic rule to perform this action;"</p> <p>Coss at 10:10-17: "1013: the remote proxy sends the packet to the firewall; based on the dynamic rule loaded in step 1012, the firewall forwards the packet to the original destination; in the case of dual reflection, the proxy uses the destination port which was determined by the firewall in step 1010, and, as the packet passes through the firewall, the IP header values are changed back to the original values."</p> <p>Coss at 10:18-21: "All future packets associated with the same session are processed alike, except that steps 1007 and 1009-1012 can be skipped. This is because the same dynamic rules apply for the life of the session."</p>
<p>[12PRE] A device for controlling data through a firewall, comprising:</p>	<p>Coss discloses and/or renders obvious a device for controlling data through a firewall.</p> <p><i>E.g.:</i></p> <p><i>See</i> [1].</p>
<p>[12A] a plurality of network interfaces, wherein each of the plurality of network interfaces is operable to</p>	<p>Coss discloses and/or renders obvious a plurality of network interfaces, wherein each of the plurality of network interfaces is operable to utilize one or more physical devices.</p> <p><i>E.g.:</i></p>

Claim	Exemplary Citation from Coss
utilize one or more physical devices;	<p>Coss at 3:25-35: "The preferred techniques can be implemented at a firewall for controlling the flow of data between, for example, separate local area networks (LANs) or subnets of a LAN. Exemplary embodiments of the invention are described herein in terms of processes. Efficient prototypes of such processes have been implemented as computer system software, using the "C" programming language for implementation on general-purpose PC hardware. Efficiency can be enhanced further, as is known, by special-purpose firmware or hardware computer system implementations."</p> <p>Coss at 3:36-4:3: "1. Support for Multiple Security Domains With a capability for supporting multiple security domains, a single firewall can support multiple users, each with a separate security policy. Also, as different security policies can apply for communications between sub-sites, such a capability can be used within a site. Respective configurations are illustrated by FIGS. 1 and 2. FIG. 1 shows four user sites 101-104, e.g., of corporations A through D, with firewall protection in their connections to the Internet 105. Such protection is provided by a firewall facility, here in the form of a LAN 110, including firewall processors 111, 113 and 114, an administrator processor 115, a router 116 and a web server 117. Each of firewall processors 113 and 114 is dedicated to a single site, namely respective sites 103 and 104. Firewall processor 111 is configured to serve the two sites 101 and 102. Firewall processor 111 implements separate firewall policies for each of the two sites vis-a-vis the Internet 105, as well as for communications between the two sites. A process for preferred operation of the firewall processor 111 is described below with reference to FIGS. 5A and 5B, including properly selecting among different firewall policies. FIG. 2 shows a user site 201 connected to the Internet 105 via a firewall processor 211. An administrator processor 215 and a router 216 are connected to the firewall processor 211. The router 216 is connected to additional firewall processors 212 and 213 which are internal to the user site 201. The firewall processor 212 protects a single sub-site 223, such as Human Resources (HR). The firewall processor 213 is configured for protecting two sub-sites, such as Payroll (P) and Disbursements (D), vis-a-vis the remainder of the site 201 as well as with respect to communications between sub-sites 221 and 222. This can be achieved by employing the process illustrated by FIGS. 5A and 5B in the firewall processor 213."</p>

Claim	Exemplary Citation from Coss
	<p>Coss at 6:3-17: "In the firewall, a decision module or engine, here called a "domain support engine" (DSE) determines which security policy to use for a new network session. Each new session must be approved by the security policies of the source domain and the destination domain(s). For connections going to the Internet, it is likely that only a single domain check is performed. The DSE makes the domain selection based on the incoming or outgoing network interface, as well as on the source or destination network address of each packet. Inclusion, in packets, of source or destination addresses allows for multiple users to be supported by a single network interface. The incoming or outgoing network interface may be in the form of a network interface card (NIC), e.g., an Intel EtherExpress Pro 100B card available from Intel Corporation."</p> <p>Coss at 6:18-28: "FIGS. 5A and 5B illustrate over-all flow for packet processing by a firewall which supports multiple domains. Such processing includes determining the domains which the packet is to cross, examining the applicable rules to ascertain whether the packet may pass, and determining whether any special processing is required. In the firewall, each domain is associated with one or more network interfaces. Interfaces that support more than one domain are separated using an IP address range to distinguish the packets. The following steps are included:"</p> <p>Coss at 7:10-15: "For convenient linking of each network interface to a domain, a domain table is used. In cases where an interface is shared by multiple domains, an address range is included. This is illustrated by FIG. 6 which shows non-overlapping address ranges."</p>
<p>[12B] a first computer readable storage medium storing a set of firewall rules, wherein the set of firewall rules is dynamically self-configurable during runtime without operator interaction, wherein the set</p>	<p>Coss discloses and/or renders obvious a first computer readable storage medium storing a set of firewall rules, wherein the set of firewall rules is dynamically self-configurable during runtime without operator interaction, wherein the set of firewall rules comprises a plurality of chains of rules forming various paths through a hierarchical structure, and wherein the hierarchical structure comprises defined places for dynamically updating the set of firewall rules during runtime without operator interaction.</p>

Claim	Exemplary Citation from Coss
<p>of firewall rules comprises a plurality of chains of rules forming various paths through a hierarchical structure, and wherein the hierarchical structure comprises defined places for dynamically updating the set of firewall rules during runtime without operator interaction;</p>	<p><i>E.g.:</i></p> <p><i>See</i> [1B], [1D].</p>
<p>[12C] a data controlling computer program comprising data controlling computer program code stored on either the first computer readable storage medium or on a second computer readable storage medium, the data controlling computer program code being executable to:</p>	<p>Coss discloses and/or renders obvious a data controlling computer program comprising data controlling computer program code stored on either the first computer readable storage medium or on a second computer readable storage medium, the data controlling computer program code being executable.</p> <p><i>E.g.:</i></p> <p>Coss at 1:9-11: "This invention relates to the prevention of unauthorized access in computer networks and, more particularly, to firewall protection within computer networks."</p> <p>Coss at 1:14-26: "In computer networks, information is conventionally transmitted in the form of packets. Information present at one site may be accessed by or transmitted to another site at the command of the former or the latter. Thus, e.g., if information is proprietary, there is a need for safeguards against unauthorized access. To this end, techniques known as packet filtering, effected at a network processor component known as a firewall, have been developed and commercialized. At the firewall, packets are inspected and filtered, i.e., passed on or dropped depending on whether they conform to a set of predefined access rules. Conventionally, these rule sets are represented in tabular form."</p>

Claim	Exemplary Citation from Coss
	<p>Coss at 3:25-35: "The preferred techniques can be implemented at a firewall for controlling the flow of data between, for example, separate local area networks (LANs) or subnets of a LAN. Exemplary embodiments of the invention are described herein in terms of processes. Efficient prototypes of such processes have been implemented as computer system software, using the "C" programming language for implementation on general-purpose PC hardware. Efficiency can be enhanced further, as is known, by special-purpose firmware or hardware computer system implementations."</p> <p>Coss at 6:3-17: "In the firewall, a decision module or engine, here called a "domain support engine" (DSE) determines which security policy to use for a new network session. Each new session must be approved by the security policies of the source domain and the destination domain(s). For connections going to the Internet, it is likely that only a single domain check is performed. The DSE makes the domain selection based on the incoming or outgoing network interface, as well as on the source or destination network address of each packet. Inclusion, in packets, of source or destination addresses allows for multiple users to be supported by a single network interface. The incoming or outgoing network interface may be in the form of a network interface card (NIC), e.g., an Intel EtherExpress Pro 100B card available from Intel Corporation."</p> <p>Coss at 6:18-28: "FIGS. 5A and 5B illustrate over-all flow for packet processing by a firewall which supports multiple domains. Such processing includes determining the domains which the packet is to cross, examining the applicable rules to ascertain whether the packet may pass, and determining whether any special processing is required. In the firewall, each domain is associated with one or more network interfaces. Interfaces that support more than one domain are separated using an IP address range to distinguish the packets. The following steps are included:"</p>
<p>[12C(i)] define at least one node, wherein the at least one node is associated with two or more network</p>	<p>Coss discloses and/or renders obvious define at least one node, wherein the at least one node is associated with two or more network interfaces of the plurality of network interfaces.</p> <p><u>E.g.:</u></p>

Claim	Exemplary Citation from Coss
interfaces of the plurality of network interfaces; and	<i>See</i> [1A].
[12C(ii)] when a packet is received at one of the two or more network interfaces associated with the at least one node, accept or deny the packet based on a review of the set of firewall rules.	Coss discloses and/or renders obvious when a packet is received at one of the two or more network interfaces associated with the at least one node, accept or deny the packet based on a review of the set of firewall rules. <i>E.g.:</i> <i>See</i> [1C], [1D].
[13] A device according to claim 12, wherein the data controlling computer program code is further executable to, while the firewall is processing traffic through the at least one node, add a rule to the set of firewall rules, delete a rule from the set of firewall rules, or modify a rule in the set of firewall rules.	Coss discloses and/or renders obvious a device according to claim 12, wherein the data controlling computer program code is further executable to, while the firewall is processing traffic through the at least one node, add a rule to the set of firewall rules, delete a rule from the set of firewall rules, or modify a rule in the set of firewall rules. <i>E.g.:</i> <i>See</i> [2].
[14PRE] A device according to claim 12, wherein the at least one node comprises a first node, and wherein the data controlling computer program code is further executable to:	Coss discloses and/or renders obvious device according to claim 12, wherein the at least one node comprises a first node, and wherein the data controlling computer program code is further executable.e <i>E.g.:</i> <i>See</i> [3].
[14A] associate a first subset of the set of firewall	Coss discloses and/or renders obvious associate a first subset of the set of firewall rules with the first node.

Claim	Exemplary Citation from Coss
rules with the first node; and	<u>E.g.:</u> <i>See</i> [3].
[14B] if the packet is received at the first node, apply the first subset of the set of firewall rules associated with the first node.	Coss discloses and/or renders obvious if the packet is received at the first node, apply the first subset of the set of firewall rules associated with the first node. <u>E.g.:</u> <i>See</i> [3].
[15PRE] A device according to claim 14, wherein the at least one node further comprises at least two nodes including a second node, and wherein the data controlling computer program code is further executable to:	Coss discloses and/or renders obvious device according to claim 14, wherein the at least one node further comprises at least two nodes including a second node, and wherein the data controlling computer program code is further executable to. <u>E.g.:</u> <i>See</i> [4].
[15A] associate a second subset of the set of firewall rules with the second node; and	Coss discloses and/or renders obvious associate a second subset of the set of firewall rules with the second node. <u>E.g.:</u> <i>See</i> [4].
[15B] if the packet is received at the second node, apply the second subset of the set of firewall rules	Coss discloses and/or renders obvious if the packet is received at the second node, apply the second subset of the set of firewall rules associated with the second node.

Claim	Exemplary Citation from Coss
associated with the second node.	<p><i>E.g.:</i></p> <p><i>See</i> [4].</p>
[16] A device according to claim 15, wherein the first subset of the set of firewall rules is the same as or different from the second subset of the set of firewall rules.	<p>Coss discloses and/or renders obvious a device according to claim 15, wherein the first subset of the set of firewall rules is the same as or different from the second subset of the set of firewall rules.</p> <p><i>E.g.:</i></p> <p><i>See</i> [5].</p>
[17] A device according to claim 15, wherein either the first subset of the set of firewall rules or the second subset of the set of firewall rules equals the entire set of firewall rules.	<p>Coss discloses and/or renders obvious a device according to claim 15, wherein either the first subset of the set of firewall rules or the second subset of the set of firewall rules equals the entire set of firewall rules.</p> <p><i>E.g.:</i></p> <p><i>See</i> [6].</p>
[18] A device according to claim 12, wherein the data controlling computer program code is further executable to condition the packet based on the set of firewall rules.	<p>Coss discloses and/or renders obvious a device according to claim 12, wherein the data controlling computer program code is further executable to condition the packet based on the set of firewall rules.</p> <p><i>E.g.:</i></p> <p><i>See</i> [7].</p>
[19] A device according to claim 18, wherein conditioning the packet based on the set of firewall rules further comprises	<p>Coss discloses and/or renders obvious a device according to claim 18, wherein conditioning the packet based on the set of firewall rules further comprises rewriting a portion of a network packet header associated with the packet.</p>

Claim	Exemplary Citation from Coss
rewriting a portion of a network packet header associated with the packet.	<p><i>E.g.:</i></p> <p><i>See</i> [8].</p>
[20] A device according to claim 12, wherein each of the at least one node is associated with at least two network interfaces.	<p>Coss discloses and/or renders obvious a device according to claim 12, wherein each of the at least one node is associated with at least two network interfaces.</p> <p><i>E.g.:</i></p> <p><i>See</i> [9].</p>
[21] A device according to claim 12, wherein each of the plurality of network interfaces is connected with at least one physical device.	<p>Coss discloses and/or renders obvious a device according to claim 12, wherein each of the plurality of network interfaces is connected with at least one physical device.</p> <p><i>E.g.:</i></p> <p><i>See</i> [10].</p>
[22] A device according to claim 12, wherein each of the plurality of network interfaces is physically connected to every other network interface of the plurality of network interfaces and wherein physical connection between the plurality of network interfaces comprises indirect physical connection between the	<p>Coss discloses and/or renders obvious a device according to claim 12, wherein each of the plurality of network interfaces is physically connected to every other network interface of the plurality of network interfaces and wherein physical connection between the plurality of network interfaces comprises indirect physical connection between the plurality of network interfaces.</p> <p><i>E.g.:</i></p> <p>Coss at 3:43-57: "FIG. 1 shows four user sites 101-104, e.g., of corporations A through D, with firewall protection in their connections to the Internet 105. Such protection is provided by a firewall facility, here in the form of a LAN 110, including firewall processors 111, 113 and 114, an administrator processor 115, a router 116 and a web server 117. Each of firewall processors 113 and 114 is dedicated to a single site, namely respective sites 103 and 104. Firewall processor 111 is configured to serve the two sites 101 and 102. Firewall processor 111 implements separate firewall policies for each of the two sites vis-a-</p>

Claim	Exemplary Citation from Coss
<p>plurality of network interfaces.</p>	<p>vis the Internet 105, as well as for communications between the two sites. A process for preferred operation of the firewall processor 111 is described below with reference to FIGS. 5A and 5B, including properly selecting among different firewall policies."</p> <p>Coss at 3:58-4:3: "FIG. 2 shows a user site 201 connected to the Internet 105 via a firewall processor 211. An administrator processor 215 and a router 216 are connected to the firewall processor 211. The router 216 is connected to additional firewall processors 212 and 213 which are internal to the user site 201. The firewall processor 212 protects a single sub-site 223, such as Human Resources (HR). The firewall processor 213 is configured for protecting two sub-sites, such as Payroll (P) and Disbursements (D), vis-a-vis the remainder of the site 201 as well as with respect to communications between sub-sites 221 and 222. This can be achieved by employing the process illustrated by FIGS. 5A and 5B in the firewall processor 213."</p>

Claim

Exemplary Citation from Coss

Figure 1

U.S. Patent Nov. 28, 2000 Sheet 1 of 12 6,154,775

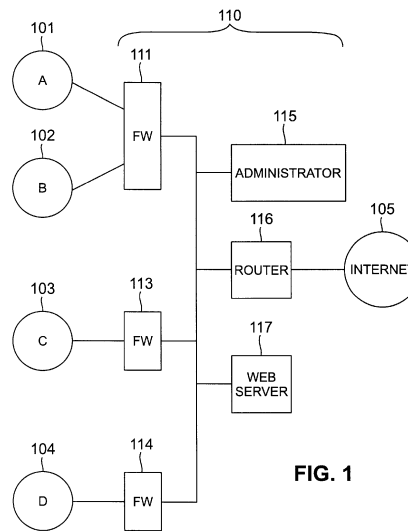
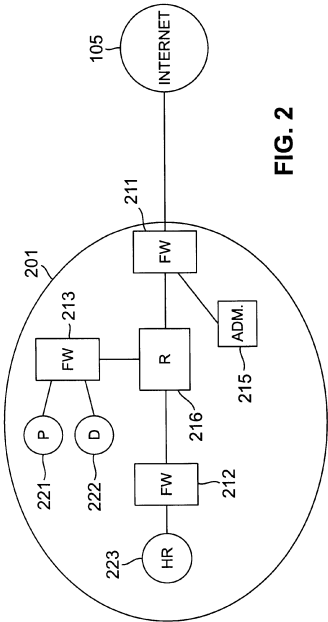


FIG. 1

Claim	Exemplary Citation from Coss
	<p data-bbox="594 237 705 264">Figure 2</p> <div data-bbox="1018 337 1486 362" style="text-align: center;"> <p>U.S. Patent Nov. 28, 2000 Sheet 2 of 12 6,154,775</p> </div>  <p data-bbox="1360 505 1388 578" style="text-align: center;">FIG. 2</p>
<p data-bbox="201 1157 548 1369">[23] A device according to claim 12, wherein the data controlling computer program code is further executable to dynamically update the set of firewall</p>	<p data-bbox="594 1157 1854 1260">Coss discloses and/or renders obvious a device according to claim 12, wherein the data controlling computer program code is further executable to dynamically update the set of firewall rules during runtime without operator interaction.</p> <p data-bbox="594 1304 667 1336"><i>E.g.:</i></p> <p data-bbox="594 1377 709 1409"><i>See [11].</i></p>

Claim	Exemplary Citation from Coss
rules during runtime without operator interaction.	
[24PRE] A data controlling computer program product comprising computer instructions stored on at least one non-transitory computer readable medium, wherein the computer instructions are operable when executed by at least one processor to:	<p>Coss discloses and/or renders obvious a data controlling computer program product comprising computer instructions stored on at least one non-transitory computer readable medium, wherein the computer instructions are operable when executed by at least one processor.</p> <p><i>E.g.:</i></p> <p><i>See</i> [1PRE].</p>
[24A] define at least one node for controlling data through a firewall, wherein at least one of the at least one node is associated with two or more network interfaces;	<p>Coss discloses and/or renders obvious to define at least one node for controlling data through a firewall, wherein at least one of the at least one node is associated with two or more network interfaces</p> <p><i>E.g.:</i></p> <p><i>See</i> [1A].</p>
[24B] associate a set of firewall rules with the at least one node, wherein the set of firewall rules further comprises a plurality of chains of rules forming various paths through a hierarchical structure, and wherein the hierarchical structure comprises defined places for dynamically	<p>Coss discloses and/or renders obvious to associate a set of firewall rules with the at least one node, wherein the set of firewall rules further comprises a plurality of chains of rules forming various paths through a hierarchical structure, and wherein the hierarchical structure comprises defined places for dynamically updating the set of firewall rules during runtime without operator interaction.</p> <p><i>E.g.:</i></p> <p><i>See</i> [1B] and [1D].</p>

Claim	Exemplary Citation from Coss
updating the set of firewall rules during runtime without operator interaction;	
[24C] receive a packet at a first node of the at least one node; and	Coss discloses and/or renders obvious to receive a packet at a first node of the at least one node <i>E.g.:</i> <i>See</i> [1C].
[24D] accept or deny the packet based on a review of the set of firewall rules, wherein the set of firewall rules is dynamically self-configurable during runtime without operator interaction.	Coss discloses and/or renders obvious to accept or deny the packet based on a review of the set of firewall rules, wherein the set of firewall rules is dynamically self-configurable during runtime without operator interaction. <i>E.g.:</i> <i>See</i> [1D].
[25] A data controlling computer program product according to claim 24, wherein the computer instructions are further executable to dynamically update the set of firewall rules during runtime without operator interaction.	Coss discloses and/or renders obvious a data controlling computer program product according to claim 24, wherein the computer instructions are further executable to dynamically update the set of firewall rules during runtime without operator interaction <i>E.g.:</i> <i>See</i> [2].
[26] A data controlling computer program product according to claim 25, wherein the computer instructions are further	Coss discloses and/or renders obvious a data controlling computer program product according to claim 25, wherein the computer instructions are further executable to, while the firewall is processing traffic through the at least one node, add a rule to the set of firewall rules, delete a rule from the set of firewall rules, or modify a rule in the set of firewall rules.

Claim	Exemplary Citation from Coss
executable to, while the firewall is processing traffic through the at least one node, add a rule to the set of firewall rules, delete a rule from the set of firewall rules, or modify a rule in the set of firewall rules.	<p><i>E.g.:</i></p> <p><i>See</i> [2].</p>
[27PRE] A data controlling computer program product according to claim 26, wherein the computer instructions are further executable to:	<p>Coss discloses and/or renders obvious a data controlling computer program product according to claim 26, wherein the computer instructions are further executable.</p> <p><i>E.g.:</i></p> <p><i>See</i> [3].</p>
[27A] associate a first subset of the set of firewall rules with the first node; and	<p>Coss discloses and/or renders obvious to associate a first subset of the set of firewall rules with the first node.</p> <p><i>E.g.:</i></p> <p><i>See</i> [3].</p>
[27B] if the packet is received at the first node, apply the first subset of the set of firewall rules associated with the first node.	<p>Coss discloses and/or renders obvious to if the packet is received at the first node, apply the first subset of the set of firewall rules associated with the first node.</p> <p><i>E.g.:</i></p> <p><i>See</i> [3].</p>
[28PRE] A data controlling computer program product according to claim 27,	<p>Coss discloses and/or renders obvious a data controlling computer program product according to claim 27, wherein the at least one node further comprises at least two nodes including a second node, and wherein the computer instructions are further executable.</p>

Claim	Exemplary Citation from Coss
<p>wherein the at least one node further comprises at least two nodes including a second node, and wherein the computer instructions are further executable to:</p>	<p><i>E.g.:</i></p> <p><i>See</i> [4].</p>
<p>[28A] associate a second subset of the set of firewall rules with the second node; and</p>	<p>Coss discloses and/or renders obvious to associate a second subset of the set of firewall rules with the second node.</p> <p><i>E.g.:</i></p> <p><i>See</i> [4].</p>
<p>[28B] if the packet is received at the second node, apply the second subset of the set of firewall rules associated with the second node.</p>	<p>Coss discloses and/or renders obvious if the packet is received at the second node, apply the second subset of the set of firewall rules associated with the second node.</p> <p><i>E.g.:</i></p> <p><i>See</i> [4].</p>
<p>[29] A data controlling computer program product according to claim 28, wherein the first subset of the set of firewall rules is the same as or different from the second subset of the set of firewall rules.</p>	<p>Coss discloses and/or renders obvious a data controlling computer program product according to claim 28, wherein the first subset of the set of firewall rules is the same as or different from the second subset of the set of firewall rules.</p> <p><i>E.g.:</i></p> <p><i>See</i> [5].</p>
<p>[30] A data controlling computer program product according to claim 28,</p>	<p>Coss discloses and/or renders obvious a data controlling computer program product according to claim 28, wherein either the first subset of the set of firewall rules or the second subset of the set of firewall rules equals the entire set of firewall rules.</p>

Claim	Exemplary Citation from Coss
<p>wherein either the first subset of the set of firewall rules or the second subset of the set of firewall rules equals the entire set of firewall rules.</p>	<p><i>E.g.:</i> <i>See</i> [6].</p>
<p>[31] A data controlling computer program product according to claim 24, wherein the computer instructions are further executable to condition the packet based on the set of firewall rules.</p>	<p>Coss discloses and/or renders obvious a data controlling computer program product according to claim 24, wherein the computer instructions are further executable to condition the packet based on the set of firewall rules.</p> <p><i>E.g.:</i> <i>See</i> [7].</p>
<p>[32] A data controlling computer program product according to claim 31, wherein conditioning the packet based on the set of firewall rules further comprises rewriting a portion of a network packet header associated with the packet.</p>	<p>Coss discloses and/or renders obvious a data controlling computer program product according to claim 31, wherein conditioning the packet based on the set of firewall rules further comprises rewriting a portion of a network packet header associated with the packet.</p> <p><i>E.g.:</i> <i>See</i> [8].</p>
<p>[33] A data controlling computer program product according to claim 24, wherein each of the at least one node comprises at least two network interfaces.</p>	<p>Coss discloses and/or renders obvious a data controlling computer program product according to claim 24, wherein each of the at least one node comprises at least two network interfaces.</p> <p><i>E.g.:</i> <i>See</i> [9].</p>

Claim	Exemplary Citation from Coss
<p>[34] A data controlling computer program product according to claim 24, wherein each of the two or more network interfaces is connected with at least one physical device.</p>	<p>Coss discloses and/or renders obvious a data controlling computer program product according to claim 24, wherein each of the two or more network interfaces is connected with at least one physical device.</p> <p><i>E.g.:</i></p> <p><i>See</i> [10].</p>
<p>[35] A data controlling computer program product according to claim 24, wherein each of the two or more network interfaces is physically connected to every other network interface of the two or more network interfaces and wherein physical connection between the two or more network interfaces comprises indirect physical connection between the two or more network interfaces.</p>	<p>Coss discloses and/or renders obvious a data controlling computer program product according to claim 24, wherein each of the two or more network interfaces is physically connected to every other network interface of the two or more network interfaces and wherein physical connection between the two or more network interfaces comprises indirect physical connection between the two or more network interfaces.</p> <p><i>E.g.:</i></p> <p><i>See</i> [22].</p>