Cisco Systems, Inc. ("Cisco") hereby contends that the asserted claims are invalid as anticipated by U.S. Patent No. 8,341,724 ("Burns") prior art references under various subsections of 35 U.S.C. § 102 and/or as obvious under 35 U.S.C. § 103 in view of the prior art reference alone, combined with the knowledge of a person of ordinary skill in the art, and/or in combination with other references in Cisco's Initial Invalidity Contentions. The chart below discloses how the prior art reference discloses, either expressly or inherently, and/or renders obvious each of the asserted claims.

The citations provided are exemplary and do not necessarily include each and every disclosure of the limitation in the references. Cisco has endeavored to cite to the most relevant portions of the identified prior art, but other portions of the identified prior art may additionally disclose, either expressly or inherently, and/or render obvious one or more limitations of the asserted claims. Thus, Cisco reserves the right to rely on: (1) uncited portions of the identified prior art; (2) other prior art not identified herein; (3) references that show the state of the art (irrespective of whether such references themselves qualify as prior art to the asserted patents); (4) factual testimony from the inventors or authors of the prior art references, or purveyors of prior art devices; and/or (5) expert testimony, to provide context to or aid in understanding the prior art and the state of the art at the time of the alleged inventions.

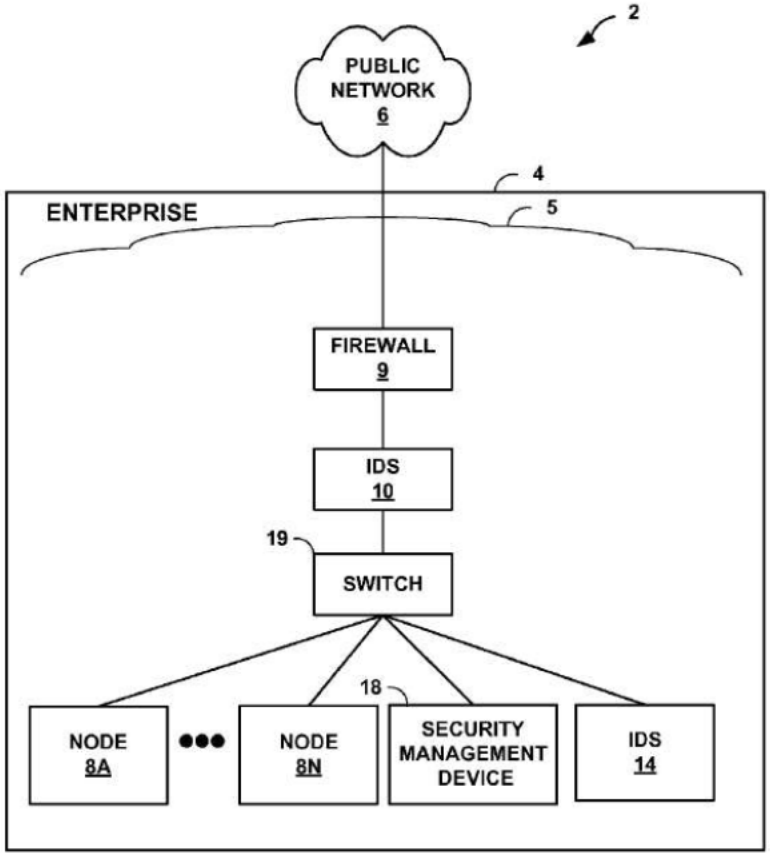
The lack of a citation for an element should not be deemed an admission that the element is not disclosed or is not inherent in the reference. When the chart indicates a particular reference discloses or embodies a limitation, the terms "discloses," "disclosed," "embodies," and "embodied" refer to explicit and/or inherent disclosure and/or obvious variations of the actual disclosure. Further, to the extent Cisco asserts that a claim is indefinite, Cisco has used its best efforts to reasonably interpret the claims to fulfill their duties in charting the prior art references.

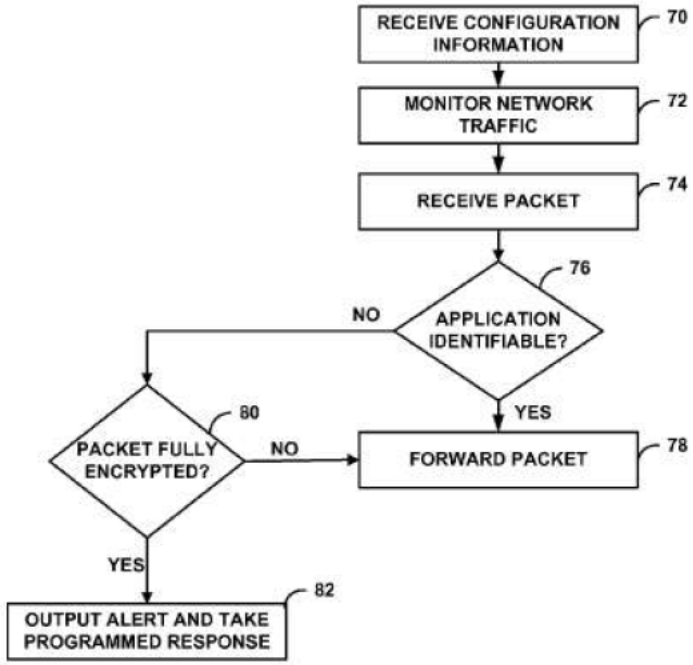
Where Cisco cites to a particular drawing or figure in the accompanying charts, the citation encompasses the description of the drawing or figure, as well as any text associated with the drawing or figure. Similarly, where Cisco cites to particular text concerning a drawing or figure, the citation encompasses that drawing or figure as well. Certain identified prior art inherently discloses features of the asserted claims. Cisco reserves the right to rely on inherency to demonstrate the invalidity of the asserted claims. Moreover, certain prior art references may inherently disclose certain features of the asserted claims as construed by Plaintiffs. Cisco may rely on cited or uncited portions of the prior art, other documents, factual testimony, and expert testimony to establish the inherency of certain features of the prior art to invalidate the asserted claims.

As set forth in Cisco's Initial Invalidity Contentions, the below contentions apply the prior art in part in accordance with Cisco's assumption that QPrivacy contends the claims are not invalid under 35 U.S.C. § 112. However, Cisco's below contentions do not represent Cisco's agreement or view as to the meaning, definiteness, written description support for, or enablement of any claim of the '249 or '824 patents, or that the '249 or '824 patents properly disclose structures corresponding to functions in any claims

governed by 35 U.S.C. § 112 ¶ 6. For each dependent claim, the disclosures cited for the claim from which it depends are incorporated by reference.

U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
1. A method of dynamic management of encrypted data during communication between a remote server and a user's device, the method comprising:	To the extent the preamble is limiting, Burns discloses this element and/or renders it obvious either alone or in combination with other references and/or the knowledge of one of ordinary skill in the art. For example, Burns describes dynamically managing encrypted data during communication between a remote server (*e.g.*, intrusion detection system (IDS)) and a user's device (*e.g.*, a "node," a security management device).

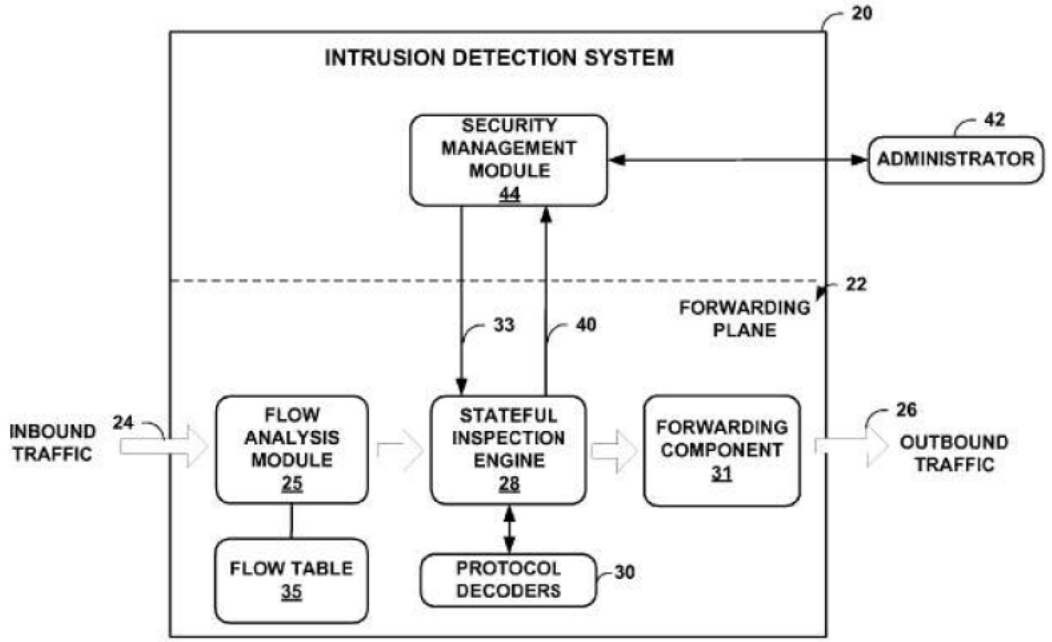
U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
	 FIG. 1 (Burns, Fig. 1.)

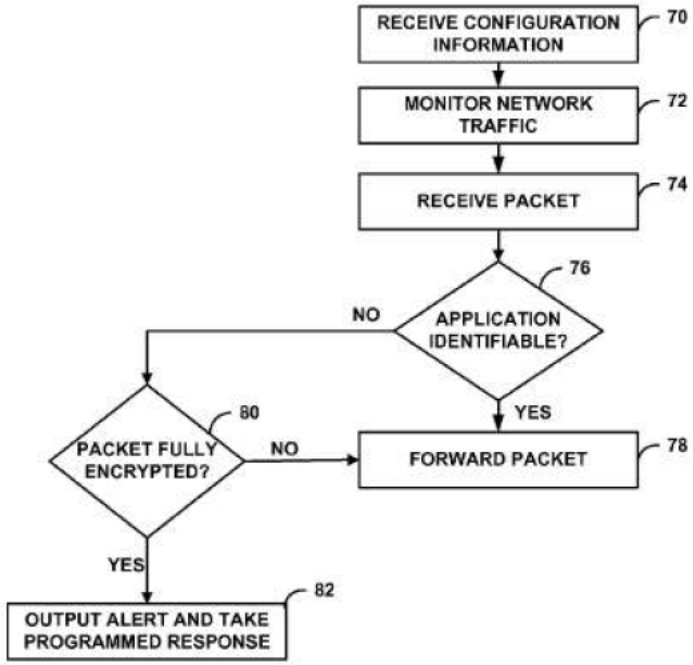
U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
	 FIG. 4 (Burns, Fig. 4.)

U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
	"Techniques are described for blocking unidentified encrypted communication sessions. In one embodiment, a device includes an interface to receive a packet, an application identification module to attempt to identify an application associated with the packet, an encryption detection module to determine whether the packet is encrypted when the application identification module is unable to identify an application associated with the packet, and an attack detection module to determine whether the packet is associated with a network attack, to forward the packet when the packet is not associated with a network attack, and to take a response when the packet is associated with a network attack, wherein the encryption detection module sends a message to the attack detection module that indicates whether the packet is encrypted, wherein when the message indicates that packet is encrypted, the attack detection module determines that the packet is associated with a network attack." (Burns, Abstract.) "FIG. 1 is a block diagram illustrating an exemplary system **2** in which enterprise computer network **4** includes intrusion detection system (IDS) **10** that intercepts packet flows associated with communication sessions and processes the packet flows to filter unwanted or malicious packet flows in accordance with the principles of the invention. In the example embodiment of FIG. 1, IDS **10** is a single network device. Network **4** also includes a private enterprise computing network **5** that is coupled to public network **6**, such as the Internet. Public network **6** may include, for example, one or more client computing devices. Firewall **9** protects enterprise network **5** and, in particular, internal computing nodes **8**A-**8**N. Computing nodes **8**A-**8**N (computing nodes **8**) represent any private computing device within enterprise network **5**, including workstations, file servers, print servers, database servers, printers and other devices. In one embodiment, IDS **10** attempts to identify applications and protocols for each communication session between computing nodes **8** and other computing devices in public network **6**. Exemplary techniques for identifying specific applications and protocols are described in greater detail in U.S. patent application Ser. No. 11/835,923, Burns et al., "Identifying Applications for Intrusion Detection Systems," filed Aug. 8, 2007, assigned to

U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
	the assignee of the present application, which is hereby incorporated by reference in its entirety." (Burns, 4:20-45.) "IDS **10** may be configurable in a variety of ways. For example, in one embodiment, IDS **10** may permit a communication session that is unencrypted to continue, despite being unable to identify a particular application that is using the communication session. In one embodiment, where IDS **10** determines that a communication session, for which an application cannot be identified, is encrypted, IDS **10** may terminate the communication session. IDS **10** may take other actions as well, such as dropping the packet, blocking future sessions from a computing device that initiated the communication session, or other actions. In one embodiment, where IDS **10** determines that a communication session, for which an application cannot be identified, is encrypted, IDS **10** may further determine whether a key exchange associated with the communication session can be identified; where a key exchange has been identified, IDS **10** may permit the communication session and where a key exchange has not been identified, IDS **10** may terminate the communication session. In one embodiment, IDS **10** may be configured to take any or all of the above actions, in accordance with a user configuration that a user, such as a system administrator, may configure." (Burns, 5:54-67.) "In some embodiments, enterprise network **5** includes multiple IDSs **10** and **14** located within different regions (e.g., sub-networks) of enterprise network **5**. Security management device **18** may operate as a central device for managing IDSs **10** and **14**. Although the example illustrated in FIG. 1 is described in terms of dedicated IDSs **10** and **14**, the functionality described herein may be incorporated within other devices, such as firewall **9** or switch **19**." (Burns, 6:9-16.) "Security management module 44 may further present a user interface by which administrator 42 may configure IDS 20 to take particular actions when a fully encrypted packet is identified. For example, the user interface may permit the administrator to drop all fully encrypted packets, log details about the communication session associated with

U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
	the fully encrypted packets, drop the packets only if a key exchange has not been previously identified for the communication session, throttle down the communication session with fully encrypted packets to reduce the bandwidth usage of that communication session, or other actions. The user interface may also enable administrator 42 to configure a randomness threshold that IDS 20 uses to determine whether a packet is encrypted, as described further herein." (Burns, 6:46-59.) "When encryption detection module determines that the packet is fully encrypted, however, ("YES" branch of **80**), encryption detection module **58** may output an alert and take a programmed response (**82**). The response to take may be in accordance with configuration data received from, e.g., administrator **42**, at step (**70**). For example, the programmed response may be to terminate the communication session, to block future communication sessions from the peer that initiated the communication session, or other actions." (Burns, 11:30-38.) *See* also Burns, 5:3-5.
1[a]. receiving, by the remote server, a communication comprising encrypted data packets;	Burns discloses this element and/or renders it obvious either alone or in combination with other references and/or the knowledge of one of ordinary skill in the art. For example, Burns discloses an IDS that receives communications comprising encrypted data packets.

U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
	 FIG. 2 (Burns, Fig. 2.)

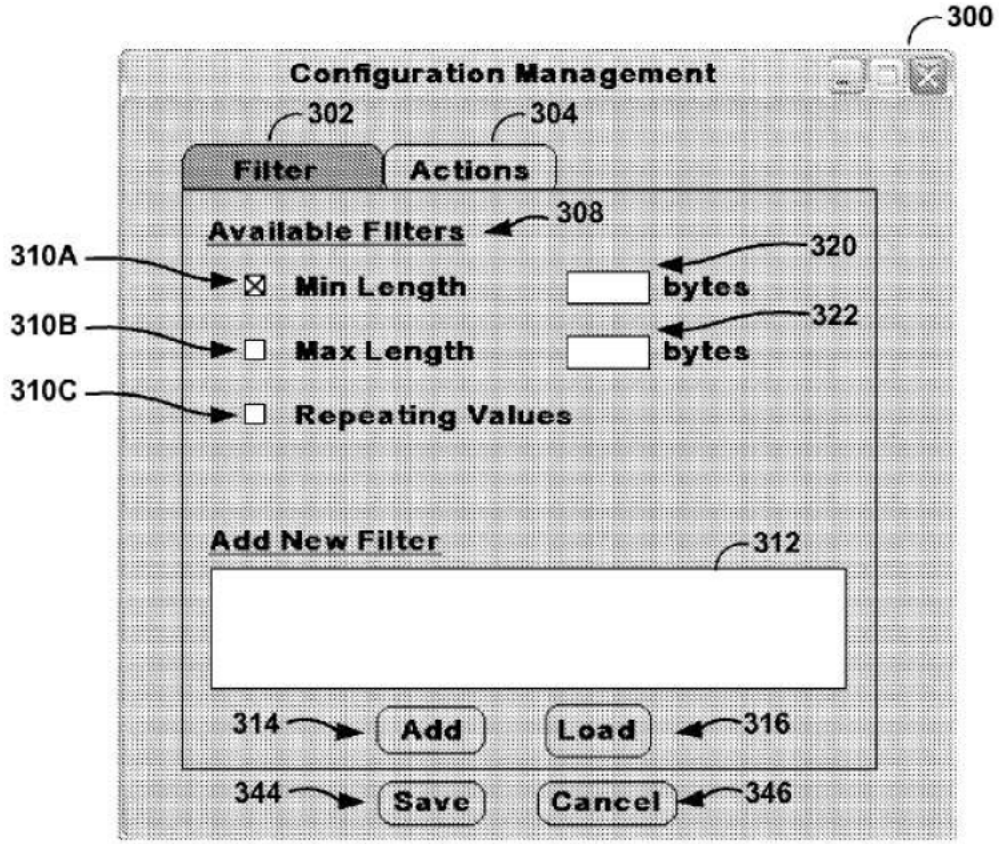
U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
	 FIG. 4 (Burns, Fig. 4.)

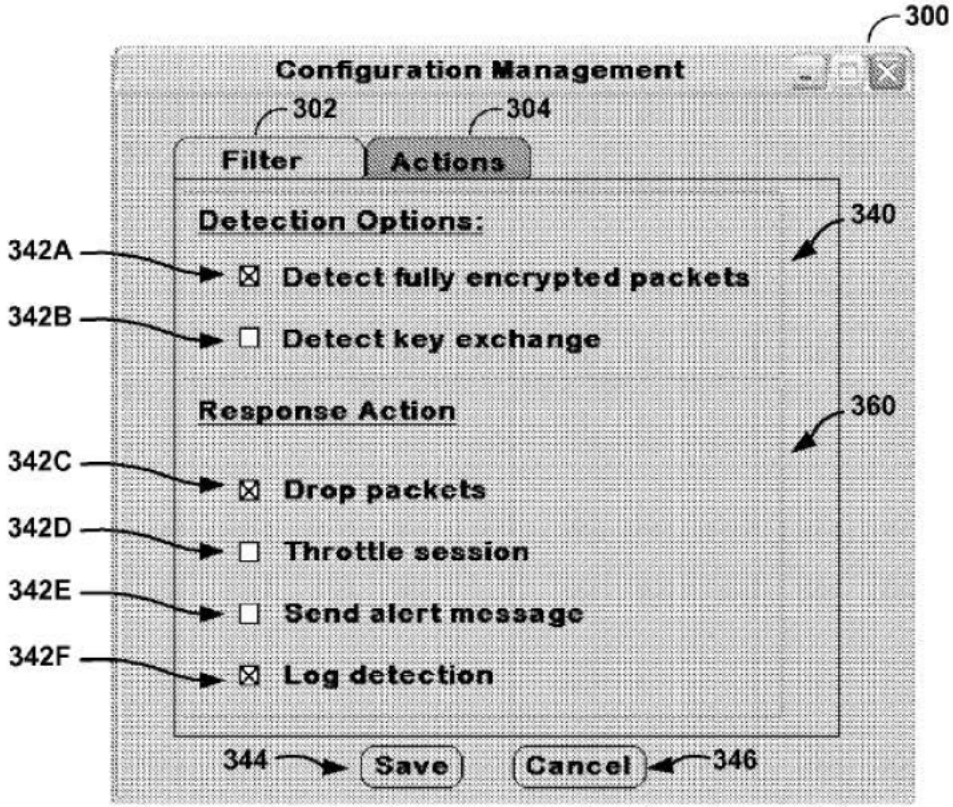
U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
	"FIG. 2 is a block diagram illustrating an example embodiment of an IDS **20**. In the illustrated example, IDS **20** includes a forwarding plane **22** that transparently monitors inbound network traffic **24** and forwards the network traffic as outbound network traffic **26**. In the example illustrated by FIG. 2, forwarding plane **22** includes flow analysis module **25**, stateful inspection engine **28**, protocol decoders **30**, forwarding component **31** and security management module **44**." (Burns, 6:29-36.) "Encryption detection module **58** attempts to determine whether the packets of the communication session are fully encrypted, i.e., that the application-layer header as well as the application-layer payload are encrypted. For example, encryption detection module **58** may extract the payload from a TCP/IP packet, which frequently includes an application-layer packet header (e.g., HTTP header) and application-layer payload. Encryption detection module **58** then analyzes characteristics of the TCP/IP payload to determine whether the payload of the TCP/IP packet is fully encrypted. That is, encryption detection module **58** examines the entire payload of a TCP/IP packet, including a region that would typically be an application-layer header, and compare characteristics of the TCP/IP payload to a randomness threshold to determine if the TCP/IP payload that would normally correspond to the application-layer header as well as the application-layer payload are encrypted." (Burns, 9:9-25.) "Once configured, IDS **20** monitors network traffic **24** (**72**). In some configurations, stateful inspection engine **28** of forwarding plane **22** may receive network traffic and mirror the network traffic for purposes of analysis. Forwarding component **31** seamlessly forwards the original network traffic. Stateful inspection engine **28** of forwarding plane **22** next receives a packet, e.g. from flow analysis module **25** (**74**). While stateful inspection engine **28** may receive all packets of a particular communication session, for the purposes of this discussion, it is assumed that this packet is the first packet following the packets used to establish the three-way

U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
	handshake of TCP/IP. In general, IDS **20** may be capable of identifying certain network attacks as early as with this first packet." (Burns, 10:18-31.) "Encryption detection module **58** inspects the packet when an application and/or protocol cannot otherwise be associated with the packet and the corresponding communication session. Encryption detection module **58** determines whether the packet is fully encrypted (**80**). That is, encryption detection module **58** examines the packet, including the application-layer header, to determine whether the packet, including the application-layer header, is encrypted. Encryption detection module **58** analyzes the TCP/IP payload of the packet to determine a randomness value of the TCP/IP payload, which includes the application-layer header as well as the application-layer payload. Where the randomness value of the packet exceeds a threshold, which may be predefined or may be configured by an administrator, encryption detection module **58** determines that the packet is encrypted." (Burns, 11:3-18.) *See* also Burns, 9:29-36.
1[b]. determining, by the remote server, a content of at least one data packet of the communication in accordance with characteristics of the at least one data packet, and wherein the content of the at least one data packet is not decrypted by the remote server, and the determination of the content is performed by the remote server in real time during a communication session between the remote server and the user's device;	Burns discloses this element and/or renders it obvious either alone or in combination with other references and/or the knowledge of one of ordinary skill in the art. For example, Burns' IDS analyzes packets to determine an application or protocol for each communication session. Burns' IDS does not decrypt encrypted packets. Burns' IDS analyzes packets in real time because it transparently monitors traffic and forwards the traffic. "As one example, the Back Orifice protocol depends upon a random number generator that is seeded, i.e. initialized, with a secret key. Both parties to a Back Orifice communication session know the secret key in advance of the communication session, and both parties have the same random number generator. By seeding the random number generator with the same secret key, both parties are able to encrypt data without exchanging a key during the communication session. In this way, the parties seek to avoid detection of any key

U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
	exchange and session establishment. Moreover, parties to the Back Orifice protocol encrypt all data in the packet, including the Back Orifice application-layer header. Back Orifice uses a 17-byte application-layer header that is encrypted, in addition to the payload, by one party and decrypted by the other party to a communication session." (Burns, 1:56-2:3.) "FIG. 1 is a block diagram illustrating an exemplary system **2** in which enterprise computer network **4** includes intrusion detection system (IDS) **10** that intercepts packet flows associated with communication sessions and processes the packet flows to filter unwanted or malicious packet flows in accordance with the principles of the invention. In the example embodiment of FIG. 1, IDS **10** is a single network device. Network **4** also includes a private enterprise computing network **5** that is coupled to public network **6**, such as the Internet. Public network **6** may include, for example, one or more client computing devices. Firewall **9** protects enterprise network **5** and, in particular, internal computing nodes **8**A-**8**N. Computing nodes **8**A-**8**N (computing nodes **8**) represent any private computing device within enterprise network **5**, including workstations, file servers, print servers, database servers, printers and other devices. In one embodiment, IDS **10** attempts to identify applications and protocols for each communication session between computing nodes **8** and other computing devices in public network **6**. Exemplary techniques for identifying specific applications and protocols are described in greater detail in U.S. patent application Ser. No. 11/835,923, Burns et al., "Identifying Applications for Intrusion Detection Systems," filed Aug. 8, 2007, assigned to the assignee of the present application, which is hereby incorporated by reference in its entirety." (Burns, 4:20-45.) "FIG. 2 is a block diagram illustrating an example embodiment of an IDS **20**. In the illustrated example, IDS **20** includes a forwarding plane **22** that transparently monitors inbound network traffic **24** and forwards the network traffic as outbound network traffic **26**. In the example illustrated by FIG. 2, forwarding plane **22** includes flow analysis

U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
	module **25**, stateful inspection engine **28**, protocol decoders **30**, forwarding component **31** and security management module **44**." (Burns, 6:29-36.) "Application identification module **51** attempts to identify an application associated with each of the intercepted communication sessions. In one embodiment, when stateful inspection engine **28** receives a packet as part of a packet flow, reassembly module **50** buffers the packet in data buffer **55**. Reassembly module **50** attempts to reconstruct application layer data from the packets in data buffer **55**. Application identification module **51** then attempts to identify the application associated with the packets in accordance with this reconstructed data. In other embodiments, application identification module **51** may use other techniques to attempt to identify the application associated with the communication session." (Burns, 8:11-23.) *See* also Burns, 5:17-20, 5:61-63, 6:30-34.
1[c]. storing, by the remote server, a preference list;	Burns discloses this element and/or renders it obvious either alone or in combination with other references and/or the knowledge of one of ordinary skill in the art. For example, Burns' IDS can be configured to match and store administrator preferences (*e.g.*, specified patterns, specified attack definitions, a specified list of permitted software applications).

U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
	 FIG. 7A (Burns, Fig. 7A.)

U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
	 FIG. 7B (Burns, Fig. 7B.)

U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
	"In certain contexts, such as within a corporate enterprise network, a system administrator or other system owner would like to restrict or limit access to and usage of network resources. For example, the system administrator may wish to prevent network access by an unknown application because the unknown application may be malware, such as a virus, trojan, or other malicious software. The system administrator may also wish to prevent users from using certain applications due to various considerations. For example, the system administrator may wish to block network access to applications such as BitTorrent, Skype, or other "grayware" applications due to consumption of network resources or security concerns with respect to the applications. Therefore, the system administrator may configure a firewall or other network device to block certain applications and protocols." (Burns, 1:21-35.) "Where IDS **10** is able to identify the application using a particular communication session, IDS **10** may either permit or prevent the communication session from continuing. For example, a system administrator may configure IDS **10** to explicitly allow all identifiable applications, allow all applications except for a specified list of identifiable applications, or prevent all communications except for communications from a specified list of permitted software applications. In cases where IDS **10** is unable to identify the application, IDS **10** may further inspect characteristics of the data from the communication session to determine whether the data is encrypted. As one example, IDS **10** may identify an encrypted communication session by determining whether the data in the communication session exceeds a randomness threshold. A system administrator may configure IDS **10** to establish or modify the randomness threshold. When the data from the communication session exceeds the randomness threshold, IDS **10** determines that the data is encrypted. Upon determining that the packet flows of the communication session are encrypted, IDS **10** applies the principles described herein to determine whether the communication session is associated with an allowed application or a typically unwanted application. For example, IDS **10** may then determine whether a proper key exchange was initially detected for the communication session and/or whether the communication

U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
	session contains fully encrypted packets or whether only application-layer data within the packets is encrypted." (Burns, 5:27-53.) "Security management module **44** presents a user interface by which administrator **42** configures IDS **20**. For example, administrator **42** may configure IDS **20** to monitor particular subnets of the enterprise network. In addition, security management module **44** presents a user interface by which administrator **42** may specify attack definitions **33**, which security management module **44** relays to stateful inspection engine **28**. In one embodiment, attack definitions **33** may be compound attack definitions. Security management module **44** may further present a user interface by which administrator **42** may configure IDS **20** to take particular actions when a fully encrypted packet is identified. For example, the user interface may permit the administrator to drop all fully encrypted packets, log details about the communication session associated with the fully encrypted packets, drop the packets only if a key exchange has not been previously identified for the communication session, throttle down the communication session with fully encrypted packets to reduce the bandwidth usage of that communication session, or other actions. The user interface may also enable administrator **42** to configure a randomness threshold that IDS **20** uses to determine whether a packet is encrypted, as described further herein." (Burns, 6:46-59.) "Initially, security management module **44** receives configuration information from administrator **42** and, in response, configures IDS **20** to monitor a network or portions thereof (subnets) of interest (**70**). During this process, configuration manager **44** presents a user interface by which administrator **42** specifies patterns or other attack definitions **33**. For example, administrator **42** may configure IDS **20** to block all packets deemed to be fully encrypted and to log information about the communication session associated with the blocked packets. Administrator **42** may also configure IDS **20** to throttle down (i.e., bandwidth limit) the communication session

U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
	associated with the packets to minimize the bandwidth used by the communication session. Administrator **42** may also configure IDS **20** to block future communication sessions from either or both of the communicating devices. IDS **20** may additionally include a default configuration that specifies actions IDS **20** should take when IDS **20** detects a fully encrypted packet. IDS **20** may, for example, be programmed to let such packets pass by default, or to block all fully encrypted packets by default." (Burns, 9:64-10:17.) *See* also Burns, 17:58-20:67. *See* also claim 4.
1[d]. determining, by the remote server, based on a comparison of the determined content, whether to modify the at least one data packet, and if so, modifying the at least one data packet; and	Burns discloses this element and/or renders it obvious either alone or in combination with other references and/or the knowledge of one of ordinary skill in the art. For example, Burns' IDS compares the application or protocol of a packet to its configuration information to determine how to handle the packet. Burns' IDS can take various actions depending on a packet's identified application or protocol, such as dropping or blocking the packet, closing the related communication session, or throttling (limiting bandwidth consumption of) the related communication session. These actions involve modification of the packets. "Where IDS **10** is able to identify the application using a particular communication session, IDS **10** may either permit or prevent the communication session from continuing. For example, a system administrator may configure IDS **10** to explicitly allow all identifiable applications, allow all applications except for a specified list of identifiable applications, or prevent all communications except for communications from a specified list of permitted software applications. In cases where IDS **10** is unable to identify the application, IDS **10** may further inspect characteristics of the data from the communication session to determine whether the data is encrypted. As one example, IDS **10** may identify an encrypted communication session by determining whether the data in the

U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
	communication session exceeds a randomness threshold. A system administrator may configure IDS **10** to establish or modify the randomness threshold. When the data from the communication session exceeds the randomness threshold, IDS **10** determines that the data is encrypted. Upon determining that the packet flows of the communication session are encrypted, IDS **10** applies the principles described herein to determine whether the communication session is associated with an allowed application or a typically unwanted application. For example, IDS **10** may then determine whether a proper key exchange was initially detected for the communication session and/or whether the communication session contains fully encrypted packets or whether only application-layer data within the packets is encrypted." (Burns, 5:27-53.) "In the event a security risk is detected, stateful inspection engine **28** outputs an alert **40** to security management module **44** for logging and further analysis. In addition, stateful inspection engine **28** may take additional actions, such as dropping the packets associated with the communication session, automatically closing the communication session, or other actions. If no security risk is detected for a given application-layer communication session, stateful inspection engine **28** instructs forwarding component **31** to forward the packet flows between the peers. Forwarding component **31** may, for example, maintain a routing table that stores routes in accordance with a topology of enterprise network **5** for use in forwarding the packet flows." (Burns, 7:45-57.) "Encryption detection module **58** attempts to determine whether the packets of the communication session are fully encrypted, i.e., that the application-layer header as well as the application-layer payload are encrypted. For example, encryption detection module **58** may extract the payload from a TCP/IP packet, which frequently includes an application-layer packet header (e.g., HTTP header) and application-layer payload. Encryption detection module **58** then analyzes characteristics of the TCP/IP payload to determine whether the payload of the TCP/IP packet is fully encrypted. That is, encryption detection module **58** examines the entire payload of a TCP/IP packet,

U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
	including a region that would typically be an application-layer header, and compare characteristics of the TCP/IP payload to a randomness threshold to determine if the TCP/IP payload that would normally correspond to the application-layer header as well as the application-layer payload are encrypted." (Burns, 9:9-25.) "In one embodiment, administrator **42** (FIG. 2) may configure a randomness threshold of IDS **20** (FIG. 2). In another embodiment, IDS **20** utilizes a randomness threshold specified by a randomness detection algorithm, such as the Wald-Wolfowitz runs test algorithm. Encryption detection module **58** determines a randomness value for a packet of the communication session being examined, i.e., the TCP/IP payload of a packet of the communication session. When the randomness value of a particular TCP/IP payload of the communication session exceeds the randomness threshold, encryption detection module **58** determines that the communication session is encrypted. Accordingly, encryption detection module **58** sends a message to attack detection module **52** that the communication session is being conducted by an undesirable application. Attack detection module **52**, therefore, may perform one or more of a variety of actions. For example, attack detection module **52** may terminate the communication session, log the communication session, generate a message for, e.g., administrator **42**, or take other actions." (Burns, 9:26-44.) "Initially, security management module **44** receives configuration information from administrator **42** and, in response, configures IDS **20** to monitor a network or portions thereof (subnets) of interest (**70**). During this process, configuration manager **44** presents a user interface by which administrator **42** specifies patterns or other attack definitions **33**. For example, administrator **42** may configure IDS **20** to block all packets deemed to be fully encrypted and to log information about the communication session associated with the blocked packets. Administrator **42** may also configure IDS **20** to throttle down (i.e., bandwidth limit) the communication session associated with the packets to minimize the bandwidth used by the communication session. Administrator **42** may also configure IDS **20** to block future communication

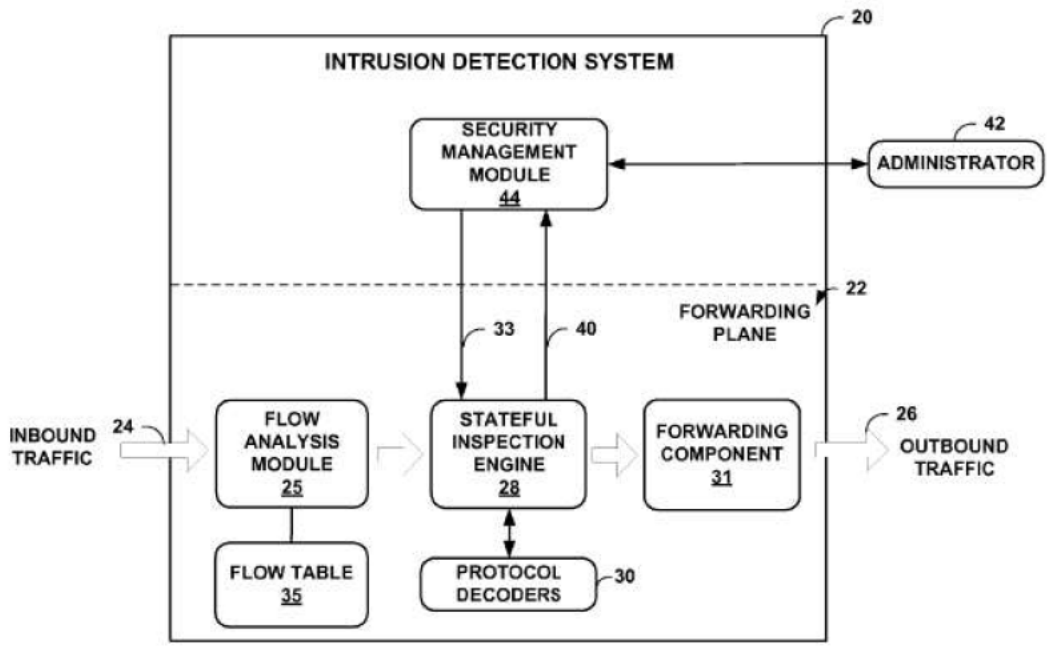
U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
	sessions from either or both of the communicating devices. IDS **20** may additionally include a default configuration that specifies actions IDS **20** should take when IDS **20** detects a fully encrypted packet. IDS **20** may, for example, be programmed to let such packets pass by default, or to block all fully encrypted packets by default." (Burns, 9:64-10:17.) *See* also claim elements 1[b] and 1[c].
1[e]. sharing, by the remote server, the modified communication.	Burns discloses this element and/or renders it obvious either alone or in combination with other references and/or the knowledge of one of ordinary skill in the art. For example, Burns' IDS shares the modified communication (communications with *e.g.*, dropped or blocked packets, a closed communication session, or throttling (limiting bandwidth consumption of)). "In the event a security risk is detected, stateful inspection engine **28** outputs an alert **40** to security management module **44** for logging and further analysis. In addition, stateful inspection engine **28** may take additional actions, such as dropping the packets associated with the communication session, automatically closing the communication session, or other actions. If no security risk is detected for a given application-layer communication session, stateful inspection engine **28** instructs forwarding component **31** to forward the packet flows between the peers. Forwarding component **31** may, for example, maintain a routing table that stores routes in accordance with a topology of enterprise network **5** for use in forwarding the packet flows." (Burns, 7:45-57.) "Initially, security management module 44 receives configuration information from administrator 42 and, in response, configures IDS 20 to monitor a network or portions thereof (subnets) of interest (120). During this process, configuration manager 44 presents a user interface by which administrator 42 specifies patterns or other attack definitions 33. For example, administrator 42 may configure IDS 20 to block all fully encrypted packets

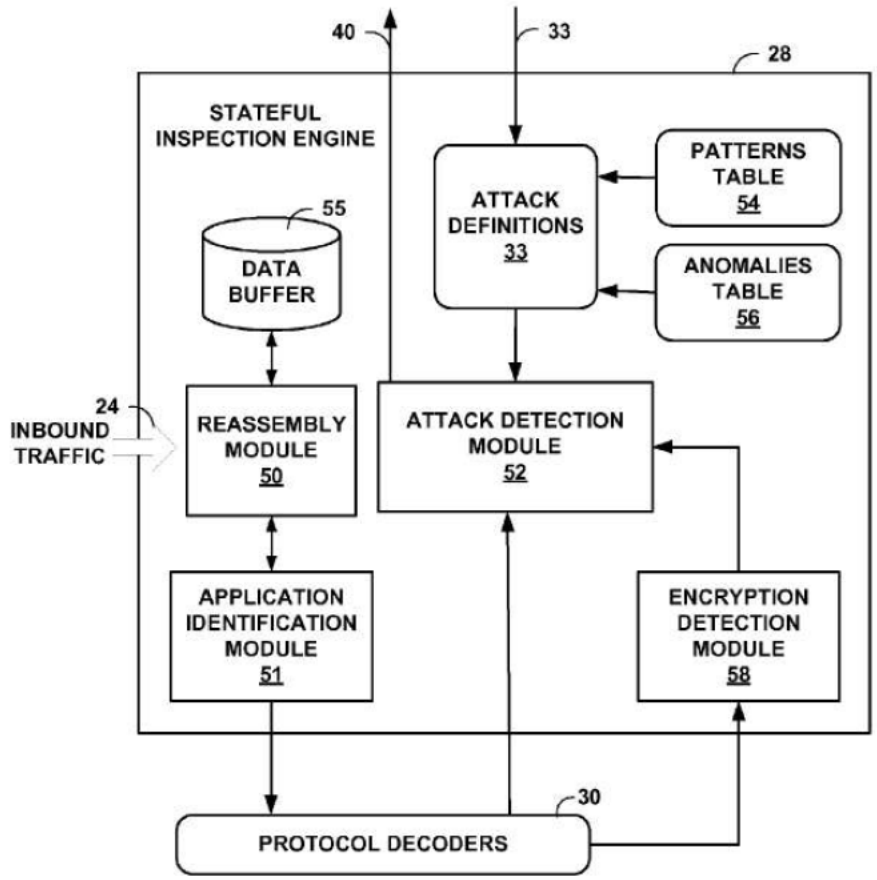
U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
	and log information about the communication session associated with the packet. Administrator 42 may also configure IDS 20 to throttle down the communication session associated with the packet to minimize the bandwidth used by the communication session. Administrator 42 may also configure IDS 20 to block future communication sessions from either or both of the communicating devices. IDS 20 may additionally include a default configuration that specifies actions IDS 20 should take when IDS 20 detects a fully encrypted packet. IDS 20 may, for example, be programmed to let such packets pass by default, or to block all fully encrypted packets by default." (Burns, 11:44-62.) *See* also claim element 1[b].
2. The method of claim 1, wherein determining a content of the at least one data packet comprises determining at least one data type of the at least one data packet of the communication in accordance with characteristics of the at least one data packet, and wherein determining whether to modify the at least one data packet is based on the determined data type.	Burns discloses this element and/or renders it obvious either alone or in combination with other references and/or the knowledge of one of ordinary skill in the art. For example, Burns' IDS analyzes packets to determine an application or protocol, which corresponds to a data type. As another example, Burns' IDS determines whether a packet is encrypted or decrypted. Encrypted and decrypted packets are associated with different data types. Burns discloses selectively modifying a packet based on whether it is encrypted. "In another embodiment, a computer-readable medium stores instructions. The computer-readable medium may be a computer-readable storage medium. The instructions cause a programmable processor to receive a network packet, determine whether the packet is associated with a network application using an application-layer header of the packet, determine whether data in the packet is encrypted, when the packet is not determined to be associated with an identifiable network application, by calculating a randomness value of the packet from a payload of the packet that includes the application-layer header and an application-layer payload and determining that the packet is encrypted when the randomness value exceeds a randomness threshold, and, when the data in the packet is determined to be encrypted, execute a response, and, when the data in the packet is determined not to be encrypted, forwarding the packet." (Burns, 3:34-49.)

U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
	"IDS **10** may be configurable in a variety of ways. For example, in one embodiment, IDS **10** may permit a communication session that is unencrypted to continue, despite being unable to identify a particular application that is using the communication session. In one embodiment, where IDS **10** determines that a communication session, for which an application cannot be identified, is encrypted, IDS **10** may terminate the communication session. IDS **10** may take other actions as well, such as dropping the packet, blocking future sessions from a computing device that initiated the communication session, or other actions. In one embodiment, where IDS **10** determines that a communication session, for which an application cannot be identified, is encrypted, IDS **10** may further determine whether a key exchange associated with the communication session can be identified; where a key exchange has been identified, IDS **10** may permit the communication session and where a key exchange has not been identified, IDS **10** may terminate the communication session. In one embodiment, IDS **10** may be configured to take any or all of the above actions, in accordance with a user configuration that a user, such as a system administrator, may configure." (Burns, 5:54-6:8.) *See* also Burns, Figs. 3, 4, 9:40-44, 11:19-22, 11:30-33, 13:5-8. *See* also claim elements 1[b] and 1[d].
3. The method of claim 2, wherein the preference list includes a list of the of forbidden and/or allowed data packet types for sharing during communication.	Burns discloses this element and/or renders it obvious either alone or in combination with other references and/or the knowledge of one of ordinary skill in the art. For example, Burns' IDS can permit or allow packets based on administrator preferences and packet characteristics such as packet application, protocol, and being encrypted/decrypted. "Where IDS **10** is able to identify the application using a particular communication session, IDS **10** may either permit or prevent the communication session from continuing. For example, a system administrator may configure IDS **10** to explicitly allow all

U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
	identifiable applications, allow all applications except for a specified list of identifiable applications, or prevent all communications except for communications from a specified list of permitted software applications. In cases where IDS **10** is unable to identify the application, IDS **10** may further inspect characteristics of the data from the communication session to determine whether the data is encrypted. As one example, IDS **10** may identify an encrypted communication session by determining whether the data in the communication session exceeds a randomness threshold. A system administrator may configure IDS **10** to establish or modify the randomness threshold. When the data from the communication session exceeds the randomness threshold, IDS **10** determines that the data is encrypted. Upon determining that the packet flows of the communication session are encrypted, IDS **10** applies the principles described herein to determine whether the communication session is associated with an allowed application or a typically unwanted application. For example, IDS **10** may then determine whether a proper key exchange was initially detected for the communication session and/or whether the communication session contains fully encrypted packets or whether only application-layer data within the packets is encrypted." (Burns, 5:27-53.) "Security management module **44** presents a user interface by which administrator **42** configures IDS **20**. For example, administrator **42** may configure IDS **20** to monitor particular subnets of the enterprise network. In addition, security management module **44** presents a user interface by which administrator **42** may specify attack definitions **33**, which security management module **44** relays to stateful inspection engine **28**. In one embodiment, attack definitions **33** may be compound attack definitions. Security management module **44** may further present a user interface by which administrator **42** may configure IDS **20** to take particular actions when a fully encrypted packet is identified. For example, the user interface may permit the administrator to drop all fully encrypted packets, log details about the communication session associated with the fully encrypted packets, drop the packets only if a key

U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
	exchange has not been previously identified for the communication session, throttle down the communication session with fully encrypted packets to reduce the bandwidth usage of that communication session, or other actions. The user interface may also enable administrator **42** to configure a randomness threshold that IDS **20** uses to determine whether a packet is encrypted, as described further herein." (Burns, 6:46-59.) "Application identification module **51** attempts to identify an application associated with the received packet (**126**). For example, application identification module **51** inspects the packet header to determine the destination port of the packet. In some cases, the destination port is associated with the protocol or application being used for the communication session. For example, port **80** is typically associated with HTTP traffic, while port **22** is typically associated with SSH traffic. Application identification module **51** may also attempt to identify an application-layer header of the packet and use the application-layer header to identify the application associated with the communication session. Application identification module **51** may use any known or future technique to attempt to determine the application associated with the communication session." (Burns, 12:7-21.) *See* also Burns, 13:9-57. *See* also claim element 1[c].
4. The method of claim 1, further comprising:	*See* claim 1.
4[a]. determining, by the remote server, at least one communication data pattern in accordance with a behavior range of the data packet, and wherein the content of the	Burns discloses this element and/or renders it obvious either alone or in combination with other references and/or the knowledge of one of ordinary skill in the art. For example, Burns' IDS identifies repeating sequences, detects encryption key exchange, and compares a packet to patterns and anomalies associated with known network attacks. As discussed with respect to claim element 1[b], the packets are not decrypted. Burns'

U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
at least one data packet is not decrypted by the remote server, and the determination of the at least one communication data pattern is performed by the remote server in real time during a communication session between the remote server and the user's device;	IDS identifies patterns using encryption detection module, which operates transparently to communications passing through the IDS.  FIG. 2 (Burns, Fig. 2.)

U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
	 FIG. 3 (Burns, Fig. 3.)

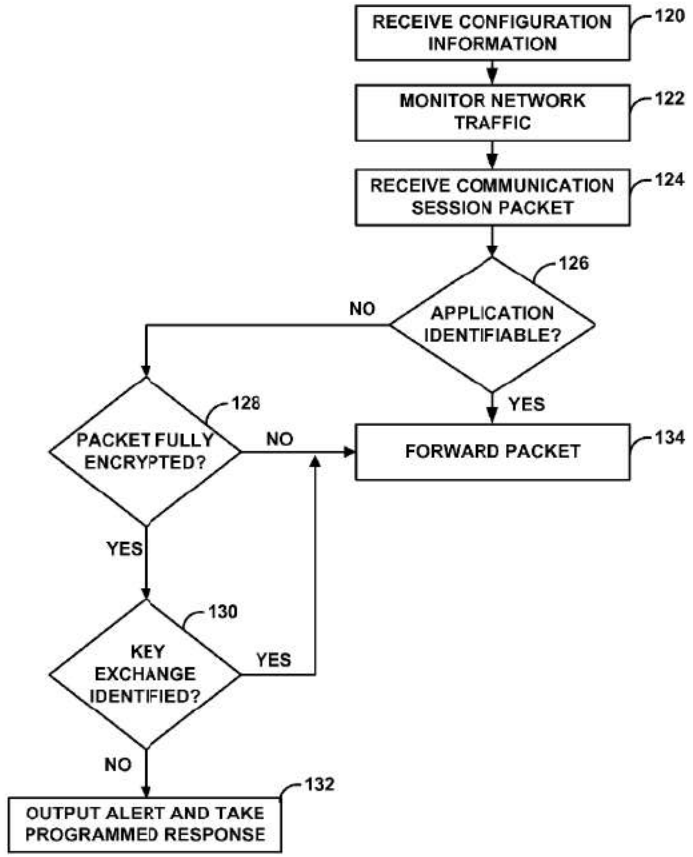
U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
	"FIG. 2 is a block diagram illustrating an example embodiment of an IDS **20**. In the illustrated example, IDS **20** includes a forwarding plane **22** that transparently monitors inbound network traffic **24** and forwards the network traffic as outbound network traffic **26**. In the example illustrated by FIG. 2, forwarding plane **22** includes flow analysis module **25**, stateful inspection engine **28**, protocol decoders **30**, forwarding component **31** and security management module **44**." (Burns, 6:29-36.) "FIG. 3 is a block diagram that illustrates an example embodiment of stateful inspection engine **28**. In the example embodiment, stateful inspection engine **28** includes reassembly module **50**, application identification module **51**, and attack detection module **52**. In addition, stateful inspection engine **28** includes patterns table **54**, data buffer **55**, anomalies table **56**, and attack definitions **33**." (Burns, 7:58-64.) "Stateful inspection engine **28** stores attack definitions **33** received from security management module **44**. Attack definitions **33** may be stored, for example, in a computer-readable medium, such as random access memory (RAM). Each of attack definitions **33** specifies a combination of one or more patterns specified within patterns table **54** and one or more protocol-specific anomalies specified within anomalies table **56**." (Burns, 8:3-10.) "When application identification module **51** is able to determine the application associated with the communication session ("YES" branch of **76**), application identification module **51** forwards the packet (**78**). In one embodiment, application identification module **51** may send the packet to protocol decoders **30** to identify the protocol in use for the communication session. In another embodiment, application identification module **51** sends the packet to attack detection module **52** to inspect the packet and to determine whether the packet is associated with a network attack. In yet another embodiment, IDS **20** simply forwards the packet towards its destination in the network." (Burns, 10:46-57.)

U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
	"Another exemplary method for determining whether a packet is encrypted includes identifying repeating patterns of varying lengths, e.g., one byte, two bytes, four bytes, or other within a packet. That is, encryption detection module **58** may determine that a packet is not random when encryption detection module **58** determines that there exist repeating patterns within the packet." (Burns, 14:32-38.) "When administrator **42** selects check box **310**A and selects save button **344**, administrator user interface **300** instructs security management module **44** to use a filter to determine whether data in a packet has repeating values. Repeated data in a packet may be an indication that the packet is not random, or that the packet is associated with a protocol that should not be blocked. In one embodiment, encryption detection module **58** compares data in the packet to other data in the packet to find a repeating sequence. In one embodiment, encryption detection module **58** stores a sequence of data from each packet in a communication session and determines whether there exists a repeated value in each packet of the communication session; in this case, the repeated value may indicate a standard header of an unknown protocol. In any case, IDS **20** may utilize a repeating values filter." (Burns, 18:30-44.) "When administrator **42** selects "Detect key exchange" check box **342**B, and then selects save button **344**, administrator user interface **300** sends a corresponding message to security management module **44**. In particular, when "Detect key exchange" check box **342**A is selected, administrator user interface **300** sends a message to security management module **44** to detect key exchanges for monitored communication sessions, or to operate in a detect key exchange mode. Accordingly, security management module **44** instructs stateful inspection engine **28** to analyze incoming packets to determine whether those packets represent a key exchange for their corresponding communication session. Stateful inspection engine **28** then begins to determine whether incoming packets represent a key exchange as part of the communication session. In one embodiment, stateful inspection engine **28** may only determine whether a first set of packets of a communication session represents a key exchange. In one

U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
	embodiment, stateful inspection engine **28** may only determine whether packets represent a key exchange when those packets correspond to a communication session for which an application and/or a protocol cannot be identified." (Burns, 19:22-42.) *See* also claim elements 1[pre] and 1[b].
4[b]. wherein the determining whether to modify the at least one data packet, by the remote server, is further based on a comparison of the determined data pattern and the preference list, whether to modify the at least one data packet, and if so, modifying the at least one data packet; and	Burns discloses this element and/or renders it obvious either alone or in combination with other references and/or the knowledge of one of ordinary skill in the art. For example, Burns' IDS uses the presence of a pattern, such as repeated data, as "an indication that the packet is not random" and "should not be blocked." Burns uses randomness to determine whether a packet is encrypted. Burns' IDS uses various criteria, including the packet being encrypted/decrypted, to determine whether to modify a packet. "Where IDS **10** is able to identify the application using a particular communication session, IDS **10** may either permit or prevent the communication session from continuing. For example, a system administrator may configure IDS **10** to explicitly allow all identifiable applications, allow all applications except for a specified list of identifiable applications, or prevent all communications except for communications from a specified list of permitted software applications. In cases where IDS **10** is unable to identify the application, IDS **10** may further inspect characteristics of the data from the communication session to determine whether the data is encrypted. As one example, IDS **10** may identify an encrypted communication session by determining whether the data in the communication session exceeds a randomness threshold. A system administrator may configure IDS **10** to establish or modify the randomness threshold. When the data from the communication session exceeds the randomness threshold, IDS **10** determines that the data is encrypted. Upon determining that the packet flows of the communication session are encrypted, IDS **10** applies the principles described herein to determine whether the communication session is associated with an allowed application or a typically unwanted application. For example, IDS **10** may then determine whether a proper key exchange was initially detected for the communication session and/or whether the communication

U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
	session contains fully encrypted packets or whether only application-layer data within the packets is encrypted." (Burns, 5:27-53.) "In one embodiment, administrator **42** (FIG. 2) may configure a randomness threshold of IDS **20** (FIG. 2). In another embodiment, IDS **20** utilizes a randomness threshold specified by a randomness detection algorithm, such as the Wald-Wolfowitz runs test algorithm. Encryption detection module **58** determines a randomness value for a packet of the communication session being examined, i.e., the TCP/IP payload of a packet of the communication session. When the randomness value of a particular TCP/IP payload of the communication session exceeds the randomness threshold, encryption detection module **58** determines that the communication session is encrypted. Accordingly, encryption detection module **58** sends a message to attack detection module **52** that the communication session is being conducted by an undesirable application. Attack detection module **52**, therefore, may perform one or more of a variety of actions. For example, attack detection module **52** may terminate the communication session, log the communication session, generate a message for, e.g., administrator **42**, or take other actions." (Burns, 9:26-44.) "When administrator **42** selects check box **310**A and selects save button **344**, administrator user interface **300** instructs security management module **44** to use a filter to determine whether data in a packet has repeating values. Repeated data in a packet may be an indication that the packet is not random, or that the packet is associated with a protocol that should not be blocked. In one embodiment, encryption detection module **58** compares data in the packet to other data in the packet to find a repeating sequence. In one embodiment, encryption detection module **58** stores a sequence of data from each packet in a communication session and determines whether there exists a repeated value in each packet of the communication session; in this case, the repeated value may indicate a standard header of an unknown protocol. In any case, IDS **20** may utilize a repeating values filter." (Burns, 18:30-44.)

U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
	See also Burns, 6:1-8, 13:33-57, 18:30-44, 18:61-65. *See* also claim element 1[d].
4[c]. wherein the preference list includes a list of forbidden and/or allowed data packet types and communication data patterns for sharing during communication.	Burns discloses this element and/or renders it obvious either alone or in combination with other references and/or the knowledge of one of ordinary skill in the art. For example, Burns IDS can selectively permit or deny certain applications or protocols based on, for example, repeated data, encryption key exchanges, and patterns and anomalies.

U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
	 **FIG. 5** (Burns, Fig. 5.)

U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
	"Where IDS **10** is able to identify the application using a particular communication session, IDS **10** may either permit or prevent the communication session from continuing. For example, a system administrator may configure IDS **10** to explicitly allow all identifiable applications, allow all applications except for a specified list of identifiable applications, or prevent all communications except for communications from a specified list of permitted software applications. In cases where IDS **10** is unable to identify the application, IDS **10** may further inspect characteristics of the data from the communication session to determine whether the data is encrypted. As one example, IDS **10** may identify an encrypted communication session by determining whether the data in the communication session exceeds a randomness threshold. A system administrator may configure IDS **10** to establish or modify the randomness threshold. When the data from the communication session exceeds the randomness threshold, IDS **10** determines that the data is encrypted. Upon determining that the packet flows of the communication session are encrypted, IDS **10** applies the principles described herein to determine whether the communication session is associated with an allowed application or a typically unwanted application. For example, IDS **10** may then determine whether a proper key exchange was initially detected for the communication session and/or whether the communication session contains fully encrypted packets or whether only application-layer data within the packets is encrypted." (Burns, 5:27-53.) "Another exemplary method for determining whether a packet is encrypted includes identifying repeating patterns of varying lengths, e.g., one byte, two bytes, four bytes, or other within a packet. That is, encryption detection module **58** may determine that a packet is not random when encryption detection module **58** determines that there exist repeating patterns within the packet." (Burns, 14:32-38.) *See* also Burns, 6:40-45, 7:47-51, 16:43-52. *See* also claim elements 1[c] and 4[b].

U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
5. The method of claim 1, wherein the modification of the communication is selected from the group consisting of: blocking the at least one data packet that is not compatible with the preference list, data nullification, data randomization, content modification, change of encoding, change of file template, change of header, change of footer, addition of a predetermined data packet, and encryption.	Burns discloses this element and/or renders it obvious either alone or in combination with other references and/or the knowledge of one of ordinary skill in the art. For example, Burns describes selectively dropping or blocking the packet, closing the communication session, and throttling. *See* claim element 1[d].
6. The method of claim 2, wherein the data type of the at least one data packet is determined based at least in part on metadata of at least one data packet of the communication.	Burns discloses this element and/or renders it obvious either alone or in combination with other references and/or the knowledge of one of ordinary skill in the art. For example, Burns describes identifying a packet's data type based in part on a TCP port value. *See* claim element 1[b] and claim 2.
7. The method of claim 4, wherein the data pattern is determined based on communication behavior, wherein the communication behavior consists of data packet frequency, data packet size, data packet speed, data packet count, data packet ratio compared to other data type flow, data packet repetition, or data packet order.	Burns discloses this element and/or renders it obvious either alone or in combination with other references and/or the knowledge of one of ordinary skill in the art. For example, Burns determines data pattern (*e.g.*, repeating pattern/sequence/value, encryption key exchange) in multiple ways, as discussed with respect to claim 4. *See* claim 4. *See* also Burns, Fig. 5, 5:64-6:4, 7:32-36, 8:59-64.
8. The method of claim 1, further comprising, the remote server	Burns discloses this element and/or renders it obvious either alone or in combination with other references and/or the knowledge of one of ordinary skill in the art.

U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
maintaining communication between the remote server and the user's device by sharing of the modified communication.	For example, Burns' IDS operates transparently and forwards modified network traffic. *See* also Burns, 7:17-19. *See* claim elements 1[b] and 1[e].
9. The method of claim 1, wherein the data type is determined based on data packet characteristics selected from a group consisting of: data packet header, data packet footer, version number, IP (Internet Protocol) address, HTTPS (HyperText Transfer Protocol Secure), file extension, encryption method, encoding method, keywords, driver, and communication protocol.	Burns discloses this element and/or renders it obvious either alone or in combination with other references and/or the knowledge of one of ordinary skill in the art. For example, Burns determines a packet's content by comparing a TCP port value to a list of known applications. *See* claim element 1[b] and claim 2.
10. The method of claim 1, wherein the remote server is a gatekeeper server.	Burns discloses this element and/or renders it obvious either alone or in combination with other references and/or the knowledge of one of ordinary skill in the art. For example, Burns' IDS "intercepts packet flows" and "filter[s] unwanted or malicious packet flows" by monitors network traffic flowing in both directions between a client and server. "FIG. 1 is a block diagram illustrating an exemplary system **2** in which enterprise computer network **4** includes intrusion detection system (IDS) **10** that intercepts packet flows associated with communication sessions and processes the packet flows to filter unwanted or malicious packet flows in accordance with the principles of the invention. In the example embodiment of FIG. 1, IDS **10** is a single network device. Network **4** also

U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
	includes a private enterprise computing network **5** that is coupled to public network **6**, such as the Internet. Public network **6** may include, for example, one or more client computing devices. Firewall **9** protects enterprise network **5** and, in particular, internal computing nodes **8**A-**8**N. Computing nodes **8**A-**8**N (computing nodes **8**) represent any private computing device within enterprise network **5**, including workstations, file servers, print servers, database servers, printers and other devices. In one embodiment, IDS **10** attempts to identify applications and protocols for each communication session between computing nodes **8** and other computing devices in public network **6**. Exemplary techniques for identifying specific applications and protocols are described in greater detail in U.S. patent application Ser. No. 11/835,923, Burns et al., "Identifying Applications for Intrusion Detection Systems," filed Aug. 8, 2007, assigned to the assignee of the present application, which is hereby incorporated by reference in its entirety." (Burns, 4:20-45.) *See* also Burns, 7:8-15, 8:59-64.
11. The method of claim 2, further comprising, the remote server issuing an alert to the user device based on the comparison of the determined data type and the preference list.	Burns discloses this element and/or renders it obvious either alone or in combination with other references and/or the knowledge of one of ordinary skill in the art. For example, Burns describes taking actions, such as issuing an alert, based on the packet's data type and the administrator-provided configuration. "Where stateful inspection engine **28** is unable to determine an identity of an application associated with a packet flow, stateful inspection engine **28** performs additional analysis on the packet flow. In one embodiment, for example, stateful inspection engine **28** attempts to determine whether the packet flow is encrypted. When stateful inspection engine **28** determines that the packet flow is encrypted, stateful inspection engine **28** further determines whether characteristics of the communication session indicates that the packet flow is associated with an unwanted software application. Stateful inspection engine **28** may, in one embodiment, determine whether a key exchange has

U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
	occurred for the communication session when stateful inspection engine **28** identifies an encrypted packet of the communication session. In this embodiment, when stateful inspection engine **28** determines that a key exchange has occurred, stateful inspection engine **28** permits the communication session to continue, but when stateful inspection engine **28** determines that a key exchange has not occurred, stateful inspection engine **28** takes a programmed response, e.g., to block the communication session, block future communication sessions from a peer of the communication session, output an alert, or other actions. In the event a security risk is detected, stateful inspection engine **28** outputs an alert **40** to security management module **44** for logging and further analysis. In addition, stateful inspection engine **28** may take additional actions, such as dropping the packets associated with the communication session, automatically closing the communication session, or other actions. If no security risk is detected for a given application-layer communication session, stateful inspection engine **28** instructs forwarding component **31** to forward the packet flows between the peers. Forwarding component **31** may, for example, maintain a routing table that stores routes in accordance with a topology of enterprise network **5** for use in forwarding the packet flows." (Burns, 7:23-57.) *See* also Burns, Figs 1, 2, 11:30-33, 20:41-53. *See* also claim elements 1[d] and claim 2.
12. A method of dynamic management of encrypted data during communication between a remote server and a user's device, the method comprising:	*See* claim element 1[pre].

U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
12[a]. receiving, by the remote server, a communication comprising encrypted data packets;	*See* claim element 1[a].
12[b]. determining, by the remote server, at least one communication data pattern of at least one data packet of the communication in accordance with a behavior range of the data packet, and wherein content of the at least one data packet is not decrypted by the remote server, and the determination of the at least one data pattern is performed by the remote server in real time during a communication session between the remote server and the user's device;	*See* claim elements 1[b] and 4[a].
12[c]. storing, by the remote server, a preference list;	*See* claim element 1[c].
12[d]. determining, by the remote server, based on a comparison of the determined data pattern and the preference list, whether to modify the at least one data packet, and if so, modifying the at least one data packet; and	*See* claim elements 1[d] and 4[b].
12[e]. sharing, by the remote server, the modified communication.	*See* claim element 1[e].

U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
13. The method of claim 12, wherein the preference list includes a list of forbidden and/or allowed communication data patterns for sharing during communication.	*See* claim 4.
14. The method of claim 12, wherein the modification of the communication is selected from the group consisting of: blocking the at least one data packet that is not compatible with the preference list, data nullification, data randomization, content modification, change of encoding, change of file template, change of header, change of footer, addition of a predetermined data packet, and encryption.	*See* claim 5.
15. The method of claim 12, wherein the communication data pattern of the at least one data packet is determined based on communication behavior, wherein the communication behavior consists of data packet frequency, data packet size, data packet speed, data packet count, data packet ratio compared to other data type flow, data packet repetition, or data packet order.	*See* claim 7.

U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
16. The method of claim 12, further comprising, the remote server maintaining communication between the remote server and the user's device by sharing of the modified communication.	*See* claim 8.
17. The method of claim 12, wherein the remote server is a gatekeeper server.	*See* claim 10.
18. The method of claim 12, further comprising, the remote server issuing an alert to the user device based on the comparison of the determined data pattern and the preference list.	*See* claims 4 and 11. *See* also Burns, Figs. 5, 7B, 20:41-53.
19. A system for dynamic management of encrypted data during communication between a remote server and a user's device, the system comprising:	*See* claim element 1[pre]. *See* also Burns, 1:6-8, 4:20-25.
19[a]. a memory;	Burns discloses this element and/or renders it obvious either alone or in combination with other references and/or the knowledge of one of ordinary skill in the art. For example, Burns comprises a memory, such as "random access memory (RAM)," "a hard drive, a network drive, [or] a flash memory stick." *See* Burns, 8:4-6, 18:51-53, 21:24-31.
19[b]. a communication data type database comprising at least one	*See* claim element 1[b] and claim 2.

U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
communication data type corresponding to sharing of at least one data packet with the user's device;	*See* also Burns, 4:36-42, 9:46-10:45.
19[c]. a preference list database;	*See* claim element 1[c].
19[d]. a communication module configured to allow communication between the remote server and the at least one user's device, and	*See* claim element 1[pre]. *See* also Burns, Fig. 2, 6:61-63.
19[e]. a processor, coupled to the preference list database, wherein the processor is configured to instruct the remote server to:	Burns discloses this element and/or renders it obvious either alone or in combination with other references and/or the knowledge of one of ordinary skill in the art. For example, Burns comprises a processor coupled to a memory for storing the preference list. *See* Burns, 3:37, 21:14-23. *See* also claim element 19[c].
19[f]. determine a content of at least one data packet of the communication in accordance with characteristics of the at least one data packet, and wherein the content of the at least one data packet is not decrypted by the remote server, and the determination of the content is performed by the remote server in real time during a communication session between the remote server and the user's device,	*See* claim element 1[b].

U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
19[g]. based on a comparison of the determined content and the preference list, determine whether to modify the at least one data packet, and if so, modify the at least one data packet; and	*See* claim elements 1[c], 1[d], and 4[b].
19[h]. share the modified communication.	*See* claim element 1[e].
20. The system of claim 19, wherein determining a content of the at least one data packet comprises determining at least one data type of the at least one data packet of the communication in accordance with characteristics of the at least one data packet, and wherein determining whether to modify the at least one data packet is based on the determined data type.	*See* claim 2.
21. The system of claim 20, wherein the preference list database comprises a list of forbidden and/or allowed data packet types for sharing during communication.	*See* claim 3.
22. The system of claim 19, wherein, the processor is further configured to determine at least one communication	*See* claim 4.

U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
data pattern in accordance with a behavior range of the data packet, and wherein the content of the at least one data packet is not decrypted by the remote server, and the determination of the at least one communication data pattern is performed by the remote server in real time during a communication session between the remote server and the user's device; and wherein the determining whether to modify the at least one data packet, by the remote server, is further based on a comparison of the determined data pattern and the preference list, whether to modify the at least one data packet, and if so, modifying the at least one data packet; and wherein the preference list includes a list of forbidden and/or allowed data packet types and communication data patterns for sharing during communication.	
23. The system of claim 20, wherein the data type of the at least one data packet is determined based at least in part on metadata of at least one data packet of the communication.	*See* claim 6.

U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
24. The system of claim 22, wherein the at least one communication data pattern is determined in accordance with a behavior range of the data packet, wherein the behavior range is selected from a group consisting of: data packet frequency, data packet size, data packet speed, data packet count, data packet ratio compared to other data type flow, data packet repetition, and data packet order.	*See* claim 7.
25. The system of claim 19, wherein the modification of the communication is selected from the group consisting of blocking the at least one data packet that is not compatible with the preference list, data nullification, data randomization, content modification, change of encoding, change of file template, change of header, change of footer, addition of a predetermined data packet and encryption.	*See* claim 5.
26. The system of claim 19, wherein the remote server is configured to maintain communication between the remote server and the user's device by sharing of the modified communication.	*See* claim 8.

U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
27. The system of claim 20, wherein the data type is determined based on data packet characteristics selected from a group consisting of: data packet header, data packet footer, version number, IP (Internet Protocol) address, HTTPS (HyperText Transfer Protocol Secure), file extension, encryption method, encoding method, keywords, driver, and communication protocol.	*See* claim 9.
28. The system of claim 19, wherein the remote server is a gatekeeper server.	*See* claim 10.
29. The system of claim 20, wherein the processor is configured to issue an alert to the user device based on the comparison of the determined data type and the preference list.	*See* claim 11.
30. The system of claim 22, wherein the preference list includes a list of forbidden and/or allowed data packet types and communication data patterns for sharing during communication, and wherein, if the at least one data type of the at least one data packet is included in the list of forbidden and/or allowed data packets, the processor is configured to	Burns discloses this element and/or renders it obvious either alone or in combination with other references and/or the knowledge of one of ordinary skill in the art. For example, Burns describes various example scenarios in which the IDS would determine whether to modify a packet based solely on its determined data type, and without consideration of Burns' various pattern-based techniques. *See* claim elements 1[d] and 4[c], claims 2, 3, and 4. *See* also Burns, Figs. 4, 7A.

U.S. Patent No. 11,816,249	
Claim	**Relevant Disclosure of Burns**
determine whether to modify the at least one data packet based on the determined data type and the preference list without performing a comparison of a determined data pattern and the preference list.	

U.S. Patent No. 11,106,824	
Claim	**Relevant Disclosure of Burns**
1. A method of dynamic management of private data during communication between a remote server and a user's device, the method compromising:	To the extent the preamble is limiting, Burns discloses this element and/or renders it obvious either alone or in combination with other references and/or the knowledge of one of ordinary skill in the art. For example, Burns describes dynamically managing private network data during communication between a remote server (*e.g.*, intrusion detection system (IDS)) and a user's device (*e.g.*, a "node," a security management device). "Methods described herein may be performed in hardware, software, or any combination thereof within a network device. For example, methods described herein may be performed by an application specific integrated circuit (ASIC) or a general-purpose processor. Methods described herein may also be embodied in a computer readable medium containing instructions. Instructions embedded in a computer readable medium may cause a programmable processor, or other processor, to perform the method, e.g. when the instructions are executed. A computer readable medium may be a computer readable storage medium. Computer readable storage media may include, for example, random access memory (RAM), read only memory (ROM), programmable read only memory (PROM), erasable programmable read only memory (EPROM), electronically erasable programmable read only memory (EEPROM), flash memory, a hard disk, a CD-ROM, a floppy disk, a cassette, magnetic media, optical media, or other computer readable media." (Burns, 21:14-31.) *See* also Burns, claim 1. *See* also claim element 17[pre].
1[a]. receiving, by the user's device, a request for retrieval of at least one data packet from the user's device, wherein the user's device is	Burns discloses this element and/or renders it obvious either alone or in combination with other references and/or the knowledge of one of ordinary skill in the art. For example, Burns discloses analyzing HTTP traffic, which includes webpage traffic. The webpages may request a user for an input.

U.S. Patent No. 11,106,824	
Claim	**Relevant Disclosure of Burns**
configured to provide a response corresponding to the received request;	"Application identification module **51** attempts to identify an application associated with the received packet (**76**). For example, application identification module **51** may inspect the packet header to determine the destination port of the packet. In some cases, the destination port is associated with the protocol or application being used for the communication session. For example, port **80** is typically associated with HTTP traffic, while port **22** is typically associated with SSH traffic. Application identification module **51** may also inspect an application-layer header, within a TCP/IP payload of the packet, to identify the application associated with the packet. Application identification module **51** may use any known or future technique to attempt to identify the application associated with the communication session." (Burns, 10:32-45.) *See* also claim 19.
1[b]. determining, by the remote server, at least one communication data type of the at least one data packet corresponding to the received request, wherein the at least one communication data type is determined in accordance with characteristics of the communication data packet, and wherein the content of the at least one data packet is not read by the remote server for continued operation by the user's device in real time during communication between the remote server and the user's device;	Burns discloses this element and/or renders it obvious either alone or in combination with other references and/or the knowledge of one of ordinary skill in the art. For example, Burns' IDS identifies an application or protocol of packets passing through it. For instance, Burns' IDS may identify the packets associated with the request for user input using the HTTP application or protocol. The IDS performs packet processing operations in real time (*e.g.*, the IDS "transparently monitors… and forwards"). The packets are not read because they are not decrypted. *See* claim element 17[e].
1[c]. receiving, by the user's device, a privacy preference for the user's	Burns discloses this element and/or renders it obvious either alone or in combination with other references and/or the knowledge of one of ordinary skill in the art.

U.S. Patent No. 11,106,824	
Claim	**Relevant Disclosure of Burns**
device, wherein the privacy preference comprises a list of allowed data packet communication types for sharing during communication;	For example, Burns' IDS handles packets, including encrypted packets, according to configuration by an administrative user (*e.g.*, determining whether to allow the packets). Burns discloses a user interface through which the administrative user provides IDS configuration information.