

Invalidity Contentions for U.S. Patent No. 8,955,038
Based on U.S. Patent No. 8,065,712 to Cheng et al. (“Cheng”)

Based upon Plaintiff's Complaint, Infringement Contentions, and apparent claim constructions and application of the claims to Defendant's accused products, as best as they can be deciphered, the reference charted below anticipates or at least renders obvious the asserted claims. These invalidity contentions are not an admission by Defendant that the accused products are covered by or infringe the asserted claims, particularly when these claims are properly construed and applied. These invalidity contentions are not an admission that Defendant concedes or acquiesces to any claim construction implied or suggested by Plaintiff's Complaint or Infringement Contentions. Nor is Defendant asserting any claim construction positions through these charts, including whether the preamble is a limitation. The portions of the prior art reference cited below are not exhaustive but are exemplary in nature.

U.S. Patent No. 8,065,712 to Cheng et al. (“Cheng”) was filed on May 25, 2005, issued on November 22, 2011, and claims priority to U.S. Provisional Patent Application No. 60/653,715 filed on February 16, 2005. This patent is prior art under at least 35 U.S.C. § 102(e), and 103(a). As described in the following claim chart, the asserted claims of U.S. Patent No. 8,955,038 (the “’038 Patent”), are invalid as anticipated by Cheng.

To the extent that Cheng is found not to anticipate one or more of the asserted claims of the ’038 Patent, these claims are invalid as obvious in view of Cheng alone or in combination with other prior art references disclosed in Defendant's Invalidity Contentions and accompanying charts, including without limitation as set forth below.

EXHIBIT E – CHENG

'038 Patent	Cheng
[1P] A method for controlling the operation of an endpoint, comprising:	To the extent the preamble is limiting, Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. Specifically, Cheng teaches a method for controlling (e.g., qualifying) the operation of an endpoint (e.g., a client machine to access a network). For example, see the following passages and/or figures, as well as all related disclosures: Cheng: Cheng discloses “methods” for "qualifying a client machine to access a network . . . Client machine must pass various checks to qualify for access . . . Client machine may be redirected" (<i>A method for controlling the operation of an endpoint</i>). (Abstract). “Methods and devices for qualifying a client machine to access a network, based on policies governing required protective measures, such as virus checking and operating system updates, are disclosed. A client machine must pass various checks to qualify for access. A client machine may be redirected to remediation resources that support efforts to bring the client machine into compliance with applicable network access requirements. A policy repository is updated regularly by vendors of protective measures. An administrator establishes user roles that are mapped to policy rule sets retrieved from the policy repository. The policy rule sets govern qualification of client machines for access to the network in accordance with the roles of the users of the machines. An access server is an intermediary between a client machine and the access manager. A client agent runs on the client machine and carries out checks, and reports the results via the access server to the access manager.” (Abstract).

EXHIBIT E – CHENG

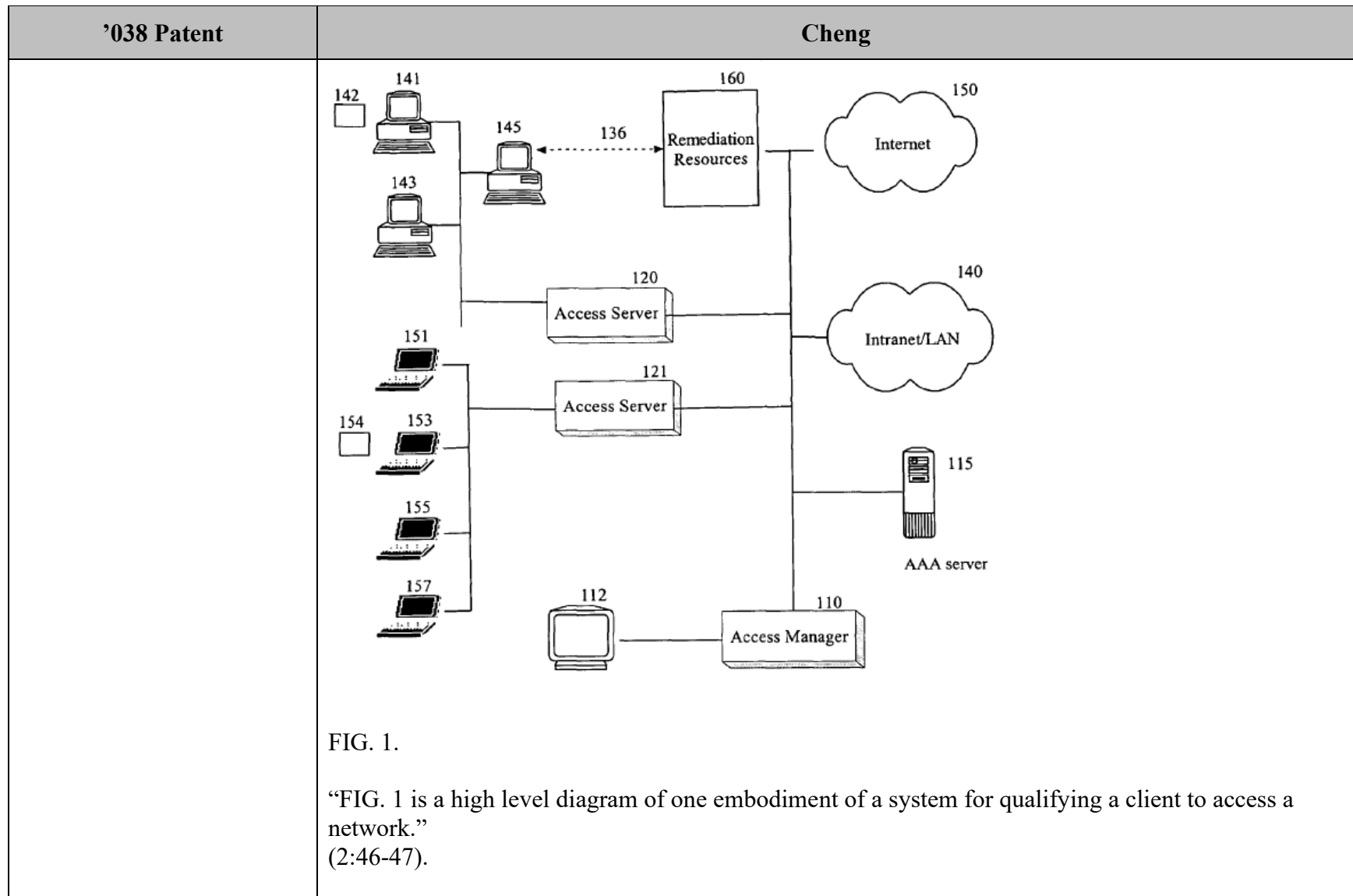


EXHIBIT E – CHENG

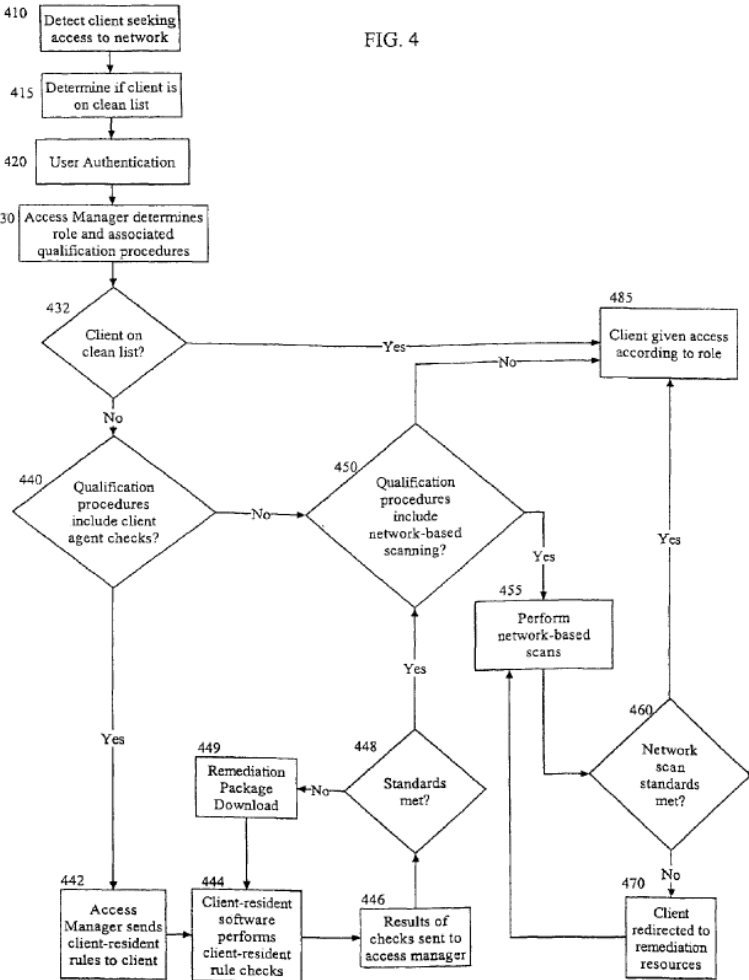
'038 Patent	Cheng
	FIG. 4  <pre> graph TD 410[410 Detect client seeking access to network] --> 415[415 Determine if client is on clean list] 415 --> 420[420 User Authentication] 420 --> 430[430 Access Manager determines role and associated qualification procedures] 430 --> 432{432 Client on clean list?} 432 -- Yes --> 485[485 Client given access according to role] 432 -- No --> 440{440 Qualification procedures include client agent checks?} 440 -- Yes --> 442[442 Access Manager sends client-resident rules to client] 442 --> 444[444 Client-resident software performs client-resident rule checks] 444 --> 446[446 Results of checks sent to access manager] 446 --> 448{448 Standards met?} 448 -- No --> 449[449 Remediation Package Download] 449 --> 444 448 -- Yes --> 450{450 Qualification procedures include network-based scanning?} 450 -- Yes --> 455[455 Perform network-based scans] 455 --> 460{460 Network scan standards met?} 460 -- No --> 470[470 Client redirected to remediation resources] 470 --> 444 460 -- Yes --> 485 450 -- No --> 485 </pre> FIG. 4. “The techniques disclosed herein integrate with an enterprise's existing authentication authority to apply role-based policy enforcement upon login to the enterprise network. Role-based policy

EXHIBIT E – CHENG

'038 Patent	Cheng
	enforcement allows access to be restricted to only applications and resources determined to be necessary to the role of the user. A web-based administrator console is used to define role-based security policies for various classes of users, from guest users, such as contractors, to system administrators, or executives of a company. For example, roles may be established such that only users with sufficient “executive” privileges, such as a Chief Financial Officer, or other executives, are allowed to access confidential financial databases. As another example, a “guest” role may be established that allows a contractor or other guest access to only public information. Based on user identifier, MAC (Media Access Control) address and IP (Internet Protocol) address, the user's role and associated privileges are tied to the specific device used to access the network.” (3:31-48). “Another type of qualification procedure is a device-based interrogation test. For this type of test, a client agent program is resident on a user's machine and used to execute the test. For example, the client agent program can scan the machine's registry for the latest virus definition files or operating system vulnerabilities. Network-based probes may not be possible on some machines due to security measures implemented by the client (such as a firewall) and/or its operating system. Device-based interrogation tests used to qualify a client machine may perform checks not possible with network-based scanning, such as detecting spyware, anti-virus software version, dates and/or versions of virus definition files, operating system update version information, etc., on the client machine.” (3:64-4:10). “The present invention relates to methods and devices for qualifying a client machine to access a network, based on policies defined by an administrator. In particular, when a client machine attempts to connect to a network, it must meet standards of adequate protection by applying various qualification procedures, such as checks performed by client agent software resident on a client machine. A client machine that fails to meet the standards of adequate protection may be redirected to remediation procedures that support efforts to bring the client machine into compliance with applicable policies.” (5:46-56).

EXHIBIT E – CHENG

'038 Patent	Cheng
	“FIG. 1 is a high level diagram of connections between various components involved in qualifying a client machine to access a network according to one embodiment. Multiple client machines 141, 143, 145, 151, 153, 155, 157 are depicted. The term ‘client machine’ as used herein is intended to broadly include any IP-enabled end station device that can access a network, such as a PC, workstation, laptop, PDA, printer, etc.” (5:57-64). “Access servers are used to enforce qualification determinations by exercising control over all packets coming from any client machine to the network.” (6:34-37). “The access manager 110 directs the qualification of a client machine through policies configured by an administrator. Details of various embodiments of the qualification process are disclosed herein.” (7:18-21). “Access may be controlled by packet filtering.” (12:67). “After any type of qualification procedures are applied, results are sent to the access manager for qualification determination. The access manager instructs one or more access servers 121, 131 regarding the results of qualifying the client for access to the network, including what type of access to enforce. Optionally, results of the qualification process may also be provided by an access server to the client.” (13:65-14:4). One of ordinary skill would find this limitation disclosed either expressly or inherently in the teachings of this reference and its incorporated disclosures taken as a whole, or in combination with the state of the art at the time of the alleged invention. To the extent this reference is not found to teach this element explicitly, implicitly, or inherently, the element would have been obvious to one of ordinary skill in the art based on this reference, common sense, ordinary creativity of one of ordinary skill in the art, and the state of the art. Additionally, it would have been obvious to combine this

EXHIBIT E – CHENG

'038 Patent	Cheng
	reference with one or more other prior art references identified in Defendant's Invalidity Contentions Cover Pleading, particularly, § IV (B). Rather than repeat those disclosures here, they are incorporated by reference into this chart.
[1A] providing a user interface, at a computing system remote from the end point, configured to allow configuration of a plurality of policies;	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. Specifically, Cheng teaches a user interface (e.g., an access manager) at a computing system remote from the end point (e.g., client machine) and configured to allow configuration of a plurality of policies (e.g., allowing the access manager to configure policy rule sets). For example, see the following passages and/or figures, as well as all related disclosures: Cheng: Cheng discloses providing “a command line or graphic user interface through administrator console 112” remote from the “client machine” (<i>providing a user interface, at a computing system remote from the endpoint</i>), at which an administrator is allowed to interact with rules manager 230 to “define role-based security policies” and “select specific [policy] rule sets for each role” (<i>user interface ... configured to allow configuration of a plurality of policies</i>). (8:27-34); (9:42-45).

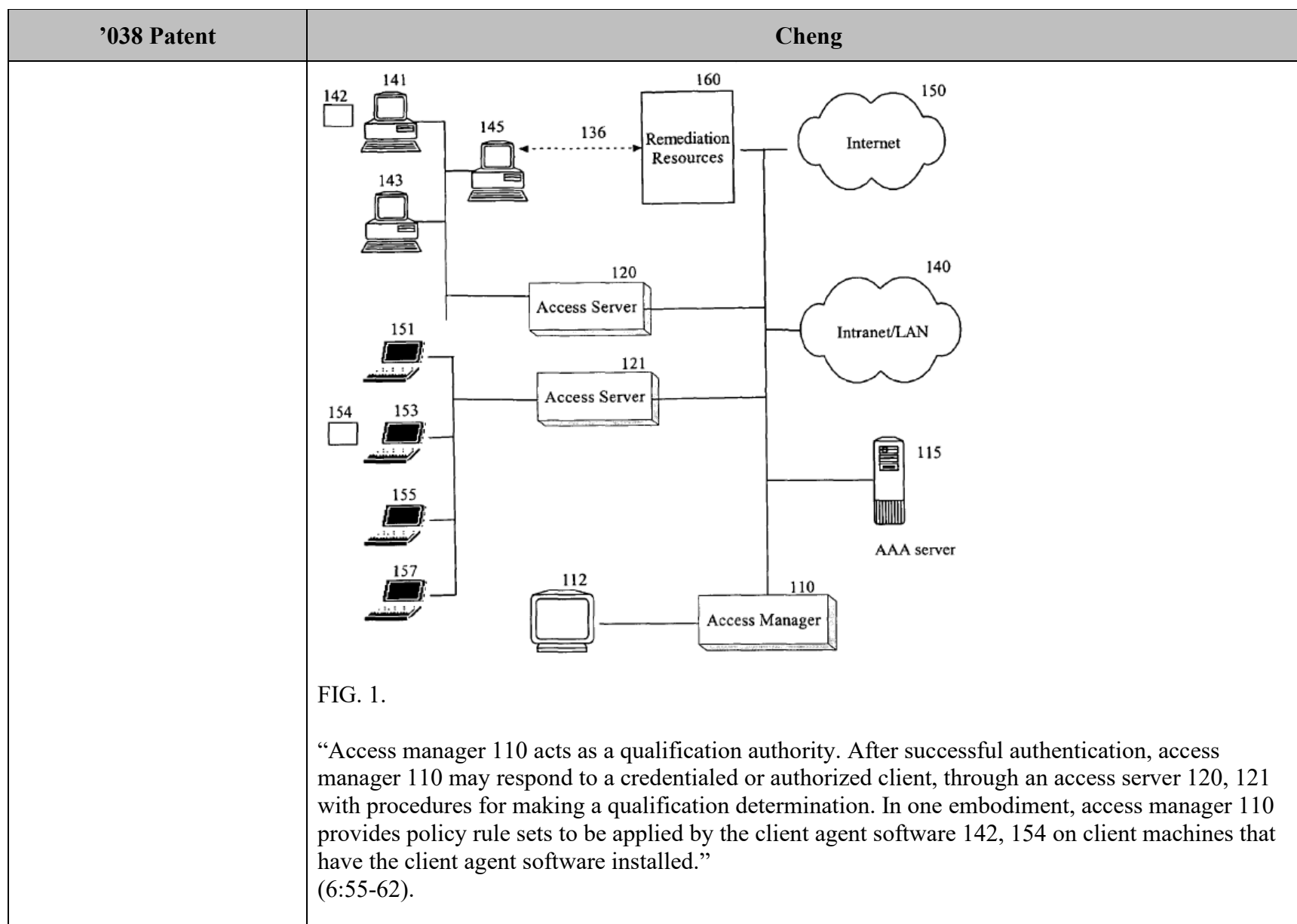


EXHIBIT E – CHENG

'038 Patent	Cheng
	“Access Manager 110 is configured and managed through administrator console 112. Preferably, administrator console 112 is a web-based application, accessible through any browser. For example, the administrator console may be a Secure Sockets Layer (SSL)-enabled browser application.” (6:63-67). “The access manager 110 directs the qualification of a client machine through policies configured by an administrator. Details of various embodiments of the qualification process are disclosed herein.” (7:18-21). “In one embodiment, the access manager 110 may be comprised of multiple functional components. FIG. 2 illustrates one embodiment of an access manager that includes a policy server 220 and a rules manager 230. Policy server 220 and rules manager 230 may run on separate servers, or separate server clusters, or they may run together on the same server or server cluster. Although only a single rules manager is shown in FIG. 2, a policy server may provide policy rule sets to many rules managers located in many different networks.” (7:23-31). “In one embodiment, a policy rule set is a collection of policy rules where each rule can be described as a Boolean expression resulting in a positive/negative outcome upon rule evaluation. Rules are typically defined to determine the posture of the client machine being assessed, including but not limited to, presence or absence of certain software, the runtime status of certain software, or whether a software module is up-to-date.” (8:27-34). “An administrator uses the rules manager to adopt and apply rule sets for a particular organization or department. Preferably, rule sets are selected and associated with roles, so that the roles can be reused and applied to particular users or user groups. The rule sets associated with a role are used to govern qualification of a client to access a network according the user's role.” (9:35-41).

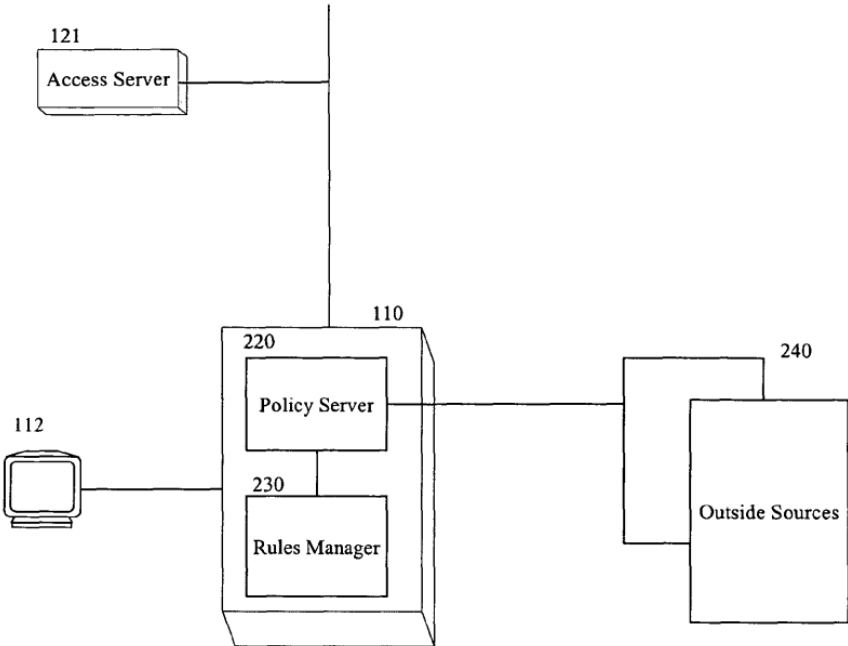
'038 Patent	Cheng
	“In one embodiment an administrator may interact with the rules manager via a command line or graphic user interface through administrator console 112 to select specific rule sets for each role. Alternatively, an automated process may be used in which certain roles may be pre-configured with associated rule sets. The administrator can use the rules manager to create roles, associate rule sets with roles, and assign prospective clients or users to roles.” (9:42-49).  FIG. 2 FIG. 2.

EXHIBIT E – CHENG

'038 Patent	Cheng
	One of ordinary skill would find this limitation disclosed either expressly or inherently in the teachings of this reference and its incorporated disclosures taken as a whole, or in combination with the state of the art at the time of the alleged invention. To the extent this reference is not found to teach this element explicitly, implicitly, or inherently, the element would have been obvious to one of ordinary skill in the art based on this reference, common sense, ordinary creativity of one of ordinary skill in the art, and the state of the art. Additionally, it would have been obvious to combine this reference with one or more other prior art references identified in Defendant's Invalidity Contentions Cover Pleading, particularly, § IV (B). Rather than repeat those disclosures here, they are incorporated by reference into this chart.
[1B] maintaining the plurality of policies in a data store on the computing system;	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. Specifically, Cheng teaches maintaining the plurality of policies in a data store on the computing system (e.g., a policy repository for storing policy rules). For example, see the following passages and/or figures, as well as all related disclosures: Cheng: Cheng discloses "a policy repository stores 'policy rules'" and "policy server 220" and "policy server may provide policy rule sets to many rules managers located in many different networks" (<i>maintaining the plurality of policies in a data store</i>) wherein the policy server 220 is part of the computing system found in FIG. 2 (<i>maintaining the plurality of policies. . .on the computing system</i>). (5:11-12); (7:24-31); and FIG. 2. “Methods and devices for qualifying a client machine to access a network, based on policies governing required protective measures, such as virus checking and operating system updates, are disclosed. A client machine must pass various checks to qualify for access. A client machine may be redirected to remediation resources that support efforts to bring the client machine into compliance with applicable network access requirements. A policy repository is updated regularly by vendors of

EXHIBIT E – CHENG

'038 Patent	Cheng
	protective measures. An administrator establishes user roles that are mapped to policy rule sets retrieved from the policy repository. The policy rule sets govern qualification of client machines for access to the network in accordance with the roles of the users of the machines. An access server is an intermediary between a client machine and the access manager. A client agent runs on the client machine and carries out checks, and reports the results via the access server to the access manager.” (Abstract). “In one embodiment, a policy repository stores ‘policy rules’ specified as combinations of conditions. The policy rules are updated regularly, such that the qualification procedures can check that the latest antivirus version has been installed on a client machine, etc. In one embodiment, the conditions generally include “checks.” A check may be a test run by web-based scanning programs and/or a test that can be executed by software resident on a client machine. In this embodiment, the checks in the policy rules are used as the qualification procedures.” (5:11-20). “A system administrator interacts with an access manager to establish user roles and select a set of policy rules and remediation procedures retrieved from the policy repository to be associated with the user roles. The access manager governs qualification of client machines for access to the network in accordance with the policy rules associated with the role of the user of the client machine.” (5:26-32). “Access manager 110 acts as a qualification authority. After successful authentication, access manager 110 may respond to a credentialed or authorized client, through an access server 120, 121 with procedures for making a qualification determination. In one embodiment, access manager 110 provides policy rule sets to be applied by the client agent software 142, 154 on client machines that have the client agent software installed.” (6:55-62). “FIG. 2 illustrates one embodiment of an access manager that includes a policy server 220 and a rules manager 230. Policy server 220 and rules manager 230 may run on separate servers, or separate server clusters, or they may run together on the same server or server cluster. Although only a single

EXHIBIT E – CHENG

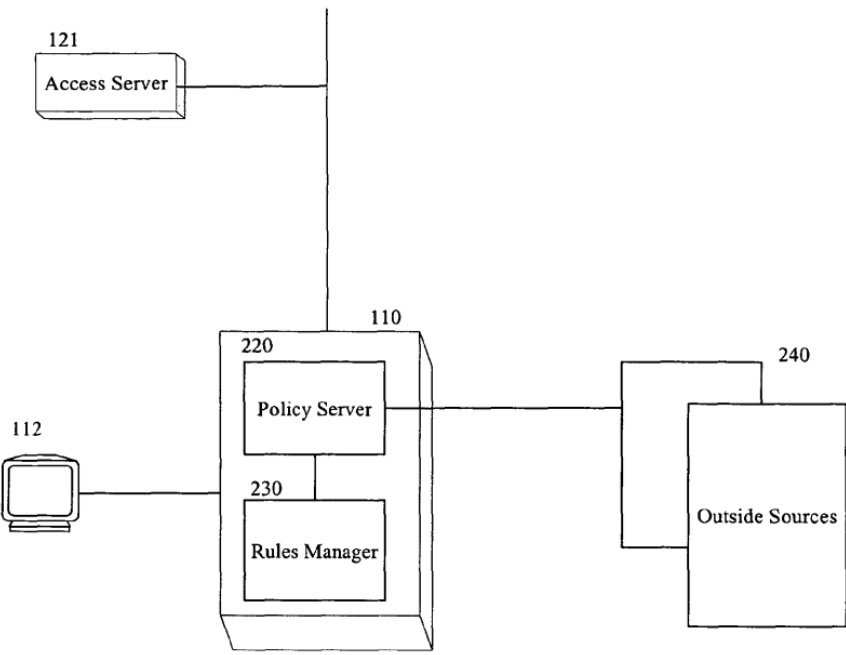
'038 Patent	Cheng
	rules manager is shown in FIG. 2, a policy server may provide policy rule sets to many rules managers located in many different networks.” (7:24-31). “The rules manager 230 receives policy rule sets from the policy server 220.” (9:24-25).  <pre> graph LR 121[Access Server] --- 110 subgraph 110 [] 220[Policy Server] 230[Rules Manager] end 112[Computer] --- 230 220 --- 240[Outside Sources] style 110 fill:none,stroke:none </pre> FIG. 2 FIG. 2.

EXHIBIT E – CHENG

'038 Patent	Cheng
	One of ordinary skill would find this limitation disclosed either expressly or inherently in the teachings of this reference and its incorporated disclosures taken as a whole, or in combination with the state of the art at the time of the alleged invention. To the extent this reference is not found to teach this element explicitly, implicitly, or inherently, the element would have been obvious to one of ordinary skill in the art based on this reference, common sense, ordinary creativity of one of ordinary skill in the art, and the state of the art. Additionally, it would have been obvious to combine this reference with one or more other prior art references identified in Defendant's Invalidity Contentions Cover Pleading, particularly, § IV (B). Rather than repeat those disclosures here, they are incorporated by reference into this chart.
[1C] identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to monitor;	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. Specifically, Cheng teaches that a plurality of operating conditions is identified from the plurality of policies (e.g., policy rule sets) and monitored on the endpoint (e.g., by the client agent software on the client machine). For example, see the following passages and/or figures, as well as all related disclosures: Cheng: Cheng discloses a "policy repository stores "policy rules specified as combinations of conditions" (<i>identifying, from the plurality of policies</i>) and that "Checks" include "application status checks, service status checks, etc." which are done on "client machines" (<i>a plurality of operating conditions on the endpoint to monitor</i>). (5:11-16); (8:39-42). “In one embodiment, a policy repository stores "policy rules" specified as combinations of conditions. The policy rules are updated regularly, such that the qualification procedures can check that the latest antivirus version has been installed on a client machine, etc. In one embodiment, the conditions generally include "checks.””

EXHIBIT E – CHENG

'038 Patent	Cheng
	(5:11-16). “Access manager 110 acts as a qualification authority. After successful authentication, access manager 110 may respond to a credentialed or authorized client, through an access server 120, 121 with procedures for making a qualification determination. In one embodiment, access manager 110 provides policy rule sets to be applied by the client agent software 142, 154 on client machines that have the client agent software installed.” (6:55-62). “Information provided by outside sources can be used to construct policy rule sets and remediation procedures. A policy rule set defines the tests that determine whether a client seeking access to the network has implemented particular protective measures. Policy rule sets further set standards for adequacy for the particular protective measures. For example, a rule set may set a standard of adequate protection for anti-virus protection, operating system update installation, worms, spyware, malware and/or adware. As additional protective measures are developed, it is anticipated that one of ordinary skill in the art will recognize how techniques disclosed herein can be adapted to include later developed protective measures. The standards of adequacy in policy rule sets are used to determine whether a client machine should be blocked from accessing the network.” (8:12-26). “In one embodiment, a policy rule set is a collection of policy rules where each rule can be described as a Boolean expression resulting in a positive/negative outcome upon rule evaluation. Rules are typically defined to determine the posture of the client machine being assessed, including but not limited to, presence or absence of certain software, the runtime status of certain software, or whether a software module is up-to-date.” (8:27-34). “Checks are atomic posture evaluation elements typically implemented through registry checks (presence/absence of registry keys, values of keys, etc.), file attribute checks, application status checks, service status checks, etc.” (8:39-42).

EXHIBIT E – CHENG

'038 Patent	Cheng
	“Rule sets may be constructed to provide different levels of network access requirements by including rules that have different qualification procedures, and/or including rules that have different standards of adequate protection. For instance, for virus checking, policy server 220 may contact multiple vendors (outside sources 240) for current engine and virus checking versions. In addition, the policy server 220 may obtain qualitative information from the virus checking vendors regarding the significance (e.g., high, medium or low) of versions of various protective measures, and use that qualitative information to establish different standards of adequate protection for different policy rule sets. For example, a rule specifying that all medium and high level virus-checking version updates must be up-to-date may be established by specifying a particular minimum version level for a particular virus-checking program as a check in a rule. This rule may then be included in a rule set.” (8:56-9:5). “At step 440, if the qualification procedures associated with the determined role include device-based interrogation tests, the process continues to step 442, where the client agent rules are sent to the client agent software resident on the client machine from the access server. The rule sets sent the client machine may be cached on the access server 121, or they may be passed through the access server 121 from access manager 110. In this case, additional rule sets may be downloaded from the access manager to the access server for future use. For example, a future client that attempts to access the network through the access server may have a different role requiring different rule sets, or the role of the current user may change.” (11:59-12:4). One of ordinary skill would find this limitation disclosed either expressly or inherently in the teachings of this reference and its incorporated disclosures taken as a whole, or in combination with the state of the art at the time of the alleged invention. To the extent this reference is not found to teach this element explicitly, implicitly, or inherently, the element would have been obvious to one of ordinary skill in the art based on this reference, common sense, ordinary creativity of one of ordinary skill in the art, and the state of the art. Additionally, it would have been obvious to combine this reference with one or more other prior art references identified in Defendant's Invalidity Contentions

EXHIBIT E – CHENG

'038 Patent	Cheng
	Cover Pleading, particularly, § IV (B). Rather than repeat those disclosures here, they are incorporated by reference into this chart.
[1D] configuring one or more software agents on the endpoint to monitor the plurality of operating conditions;	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. Specifically, Cheng teaches that software agents (e.g., client agent software) are configured on the endpoint (e.g., client machine) to apply the policy rule sets on the client machine. For example, see the following passages and/or figures, as well as all related disclosures: Cheng: Cheng discloses a "client agent software resident" (<i>one or more software agents</i>) that is "downloaded and installed on a client machine" (<i>configuring . . . on the endpoint</i>) and "can perform registry, process, application and service checks on the client machine" (<i>to monitor the plurality of operating conditions</i>). (6:2-9); (8:39-42). “Another type of qualification procedure is a device-based interrogation test. For this type of test, a client agent program is resident on a user's machine and used to execute the test. For example, the client agent program can scan the machine's registry for the latest virus definition files or operating system vulnerabilities. Network-based probes may not be possible on some machines due to security measures implemented by the client (such as a firewall) and/or its operating system. Device-based interrogation tests used to qualify a client machine may perform checks not possible with network-based scanning, such as detecting spyware, anti-virus software version, dates and/or versions of virus definition files, operating system update version information, etc., on the client machine.” (3:64-4:10). “A check may be a test run by web-based scanning programs and/or a test that can be executed by software resident on a client machine.” (5:16-18).

EXHIBIT E – CHENG

'038 Patent	Cheng
	“A further aspect of the invention is an access server that serves as an intermediary between a client machine and the access manager, and enforces network access based on the qualification determinations made by the access manager. The client agent is another aspect of the invention. The client agent comprises software resident on a client machine and carries out certain checks, as indicated by the rule set, and reports the results via the access server to the access manager. The client agent may also receive automatic updates and patches via the access server. Particular aspects of the present invention are described in the claims, specification and drawings.” (5:33-44). “In particular, when a client machine attempts to connect to a network, it must meet standards of adequate protection by applying various qualification procedures, such as checks performed by client agent software resident on a client machine.” (5:48-52). “A client machine 141, 153 may include optional client agent software 142, 154 resident on the client machine. Client agent software 142, 154, is not required, as shown by client machines 143, 145, 151, 155, 157. Not shown are various client resources available on the client machines. In general, client agent software resident on client machines provides local-machine agent-based vulnerability assessment and remediation. Once the client agent is downloaded and installed on a client machine, it can perform registry, process, application and service checks on the client machine. The results of these checks can be used to detect antivirus software installation, status and virus definition states.” (5:65-6:9). “Access manager 110 acts as a qualification authority. After successful authentication, access manager 110 may respond to a credentialed or authorized client, through an access server 120, 121 with procedures for making a qualification determination. In one embodiment, access manager 110 provides policy rule sets to be applied by the client agent software 142, 154 on client machines that have the client agent software installed.” (6:55-62).

EXHIBIT E – CHENG

'038 Patent	Cheng
	“Rules are typically defined to determine the posture of the client machine being assessed, including but not limited to, presence or absence of certain software, the runtime status of certain software, or whether a software module is up-to-date.” (8:30-34). “Checks are atomic posture evaluation elements typically implemented through registry checks (presence/absence of registry keys, values of keys, etc.), file attribute checks, application status checks, service status checks, etc.” (8:39-42). “At step 440, if the qualification procedures associated with the determined role include device-based interrogation tests, the process continues to step 442, where the client agent rules are sent to the client agent software resident on the client machine from the access server. The rule sets sent the client machine may be cached on the access server 121, or they may be passed through the access server 121 from access manager 110. In this case, additional rule sets may be downloaded from the access manager to the access server for future use. For example, a future client that attempts to access the network through the access server may have a different role requiring different rule sets, or the role of the current user may change.” (11:59-12:4). “At step 444, the client agent applies the checks in the rule sets associated with the user's determined role, and determines whether conditions defined by elements of the rule sets are true or false. For example, the registry can be scanned for the latest virus definition files or for operating system vulnerabilities, according to various checks in the rule sets.” (12:33-38). One of ordinary skill would find this limitation disclosed either expressly or inherently in the teachings of this reference and its incorporated disclosures taken as a whole, or in combination with the state of the art at the time of the alleged invention. To the extent this reference is not found to teach this element explicitly, implicitly, or inherently, the element would have been obvious to one of ordinary skill in the art based on this reference, common sense, ordinary creativity of one of ordinary

EXHIBIT E – CHENG

'038 Patent	Cheng
	skill in the art, and the state of the art. Additionally, it would have been obvious to combine this reference with one or more other prior art references identified in Defendant's Invalidity Contentions Cover Pleading, particularly, § IV (B). Rather than repeat those disclosures here, they are incorporated by reference into this chart.
[1E] receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint gathered by the one or more software agents;	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. Specifically, Cheng teaches the client agent is a software agent on a client machine that gathers status information about the plurality of operating conditions on the client machine, as defined by elements of policy rule sets, which are then reported back to the computing system, at the access manager. For example, see the following passages and/or figures, as well as all related disclosures: Cheng: Cheng discloses a "client agent" that "carries out certain checks" (<i>status information about the plurality of operating conditions on the endpoint</i>) and "reports the results via the access server to the access manager" (<i>receiving, across a network, at the computing system</i>). (5:37-40). “Methods and devices for qualifying a client machine to access a network, based on policies governing required protective measures, such as virus checking and operating system updates, are disclosed. A client machine must pass various checks to qualify for access. A client machine may be redirected to remediation resources that support efforts to bring the client machine into compliance with applicable network access requirements. A policy repository is updated regularly by vendors of protective measures. An administrator establishes user roles that are mapped to policy rule sets retrieved from the policy repository. The policy rule sets govern qualification of client machines for access to the network in accordance with the roles of the users of the machines. An access server is an intermediary between a client machine and the access manager. A client agent runs on the client machine and carries out checks, and reports the results via the access server to the access manager.” (Abstract).

EXHIBIT E – CHENG

'038 Patent	Cheng
	“A further aspect of the invention is an access server that serves as an intermediary between a client machine and the access manager, and enforces network access based on the qualification determinations made by the access manager. The client agent is another aspect of the invention. The client agent comprises software resident on a client machine and carries out certain checks, as indicated by the rule set, and reports the results via the access server to the access manager. The client agent may also receive automatic updates and patches via the access server. Particular aspects of the present invention are described in the claims, specification and drawings.” (5:33-44). “In particular, when a client machine attempts to connect to a network, it must meet standards of adequate protection by applying various qualification procedures, such as checks performed by client agent software resident on a client machine.” (5:48-52). “A client machine 141, 153 may include optional client agent software 142, 154 resident on the client machine. Client agent software 142, 154, is not required, as shown by client machines 143, 145, 151, 155, 157. Not shown are various client resources available on the client machines. In general, client agent software resident on client machines provides local-machine agent-based vulnerability assessment and remediation. Once the client agent is downloaded and installed on a client machine, it can perform registry, process, application and service checks on the client machine. The results of these checks can be used to detect antivirus software installation, status and virus definition states.” (5:65-6:9). “In order to access an internal intranet or LAN 140, the Internet 150, or any other resources available on the network, client machines must first go through access servers 120, 121. Access servers can be deployed at the edge of a network, as shown in FIG. 1, or they may be deployed centrally. For example, in a VLAN-enabled environment, multiple VLANs can be trunked through a single access server.” (6:22-28).

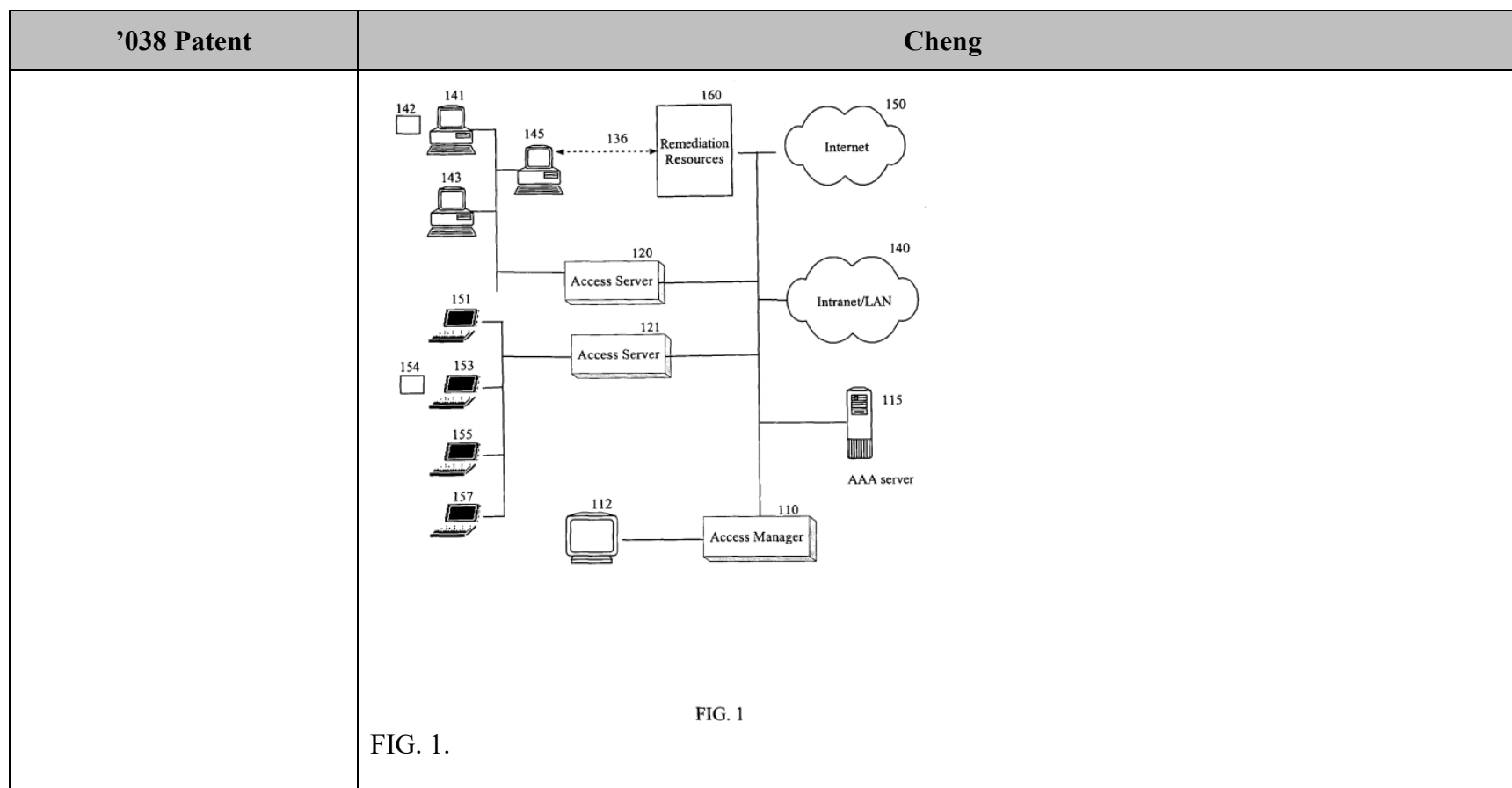
EXHIBIT E – CHENG

'038 Patent	Cheng
	“Access manager 110 acts as a qualification authority. After successful authentication, access manager 110 may respond to a credentialed or authorized client, through an access server 120, 121 with procedures for making a qualification determination. In one embodiment, access manager 110 provides policy rule sets to be applied by the client agent software 142, 154 on client machines that have the client agent software installed.” (6:55-62). “Rules are typically defined to determine the posture of the client machine being assessed, including but not limited to, presence or absence of certain software, the runtime status of certain software, or whether a software module is up-to-date.” (8:30-34). “Checks are atomic posture evaluation elements typically implemented through registry checks (presence/absence of registry keys, values of keys, etc.), file attribute checks, application status checks, service status checks, etc.” (8:39-42). “A user may enter user identification information as part of the request for access. For example, a user may enter a user identifier and a password, or use a biometric appliance. A secure web login page, or alternatively the clean agent software resident on client machines, may be used to present a login interface and obtain identification information from the user.” (11:4-10). “The role may be determined from a number of attributes. For example, the MAC address of the client machine, the subnet through which access is requested, the IP address of the client machine and the user identifier may all be used to determine a role. In one embodiment, the MAC address is given higher priority than the user identifier, such that if a user's login identifier associates him with ‘Role B’, but the MAC address associates the client with ‘Role A’, ‘Role A’ may be used instead of Role B. Other priorities may be configured.” (11:39-48).

EXHIBIT E – CHENG

'038 Patent	Cheng
	“At step 444, the client agent applies the checks in the rule sets associated with the user's determined role, and determines whether conditions defined by elements of the rule sets are true or false. For example, the registry can be scanned for the latest virus definition files or for operating system vulnerabilities, according to various checks in the rule sets.” (12:33-38). “Any results from the checks are forwarded to the access manager via the access server at step 446. The rule sets may not indicate what results of applying the checks will result in qualification to access the network. Reporting the results of the checks may simply include reporting a set of true and false indications. Alternatively, rule sets could fully describe conditions necessary for qualification and the resident client agent software could report the sum evaluation of the checks. These results are evaluated by the access manager to determine whether the checks meet the standards of adequacy set by the rule sets, as indicated by step 448.” (12:39-49).

EXHIBIT E – CHENG



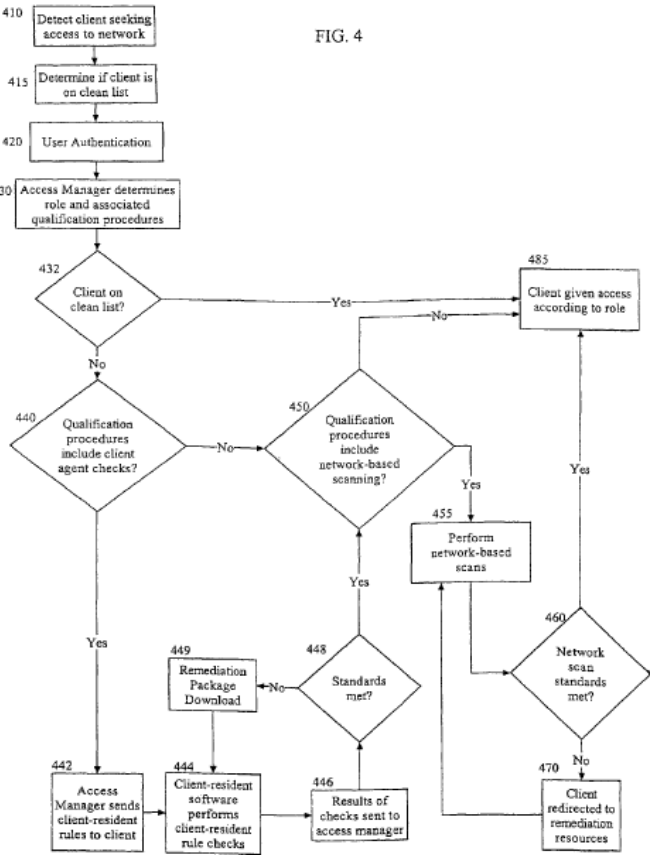
'038 Patent	Cheng
	FIG. 4  <pre> graph TD 410[410 Detect client seeking access to network] --> 415[415 Determine if client is on clean list] 415 --> 420[420 User Authentication] 420 --> 430[430 Access Manager determines role and associated qualification procedures] 430 --> 432{432 Client on clean list?} 432 -- Yes --> 485[485 Client given access according to role] 432 -- No --> 440{440 Qualification procedures include client agent checks?} 440 -- Yes --> 442[442 Access Manager sends client-resident rules to client] 442 --> 444[444 Client-resident software performs client-resident rule checks] 444 --> 446[446 Results of checks sent to access manager] 446 --> 448{448 Standards met?} 448 -- No --> 449[449 Remediation Package Download] 448 -- Yes --> 450{450 Qualification procedures include network-based scanning?} 449 --> 450 450 -- Yes --> 455[455 Perform network-based scans] 455 --> 460{460 Network scan standards met?} 460 -- No --> 470[470 Client redirected to remediation resources] 460 -- Yes --> 485 450 -- No --> 485 </pre> FIG. 4. “1. A method of qualifying a client machine to access a network, comprising the computer-implemented steps of: receiving a request for access from the client machine from an access server through which the client machine must first go to access the network, said request including user identification information;

EXHIBIT E – CHENG

'038 Patent	Cheng
	determining qualification procedures and standards of adequate protection for the client machine based on the user identification information; sending the determined qualification procedures to the access server, receiving from the access server results of applying the qualification procedures at the client machine; determining a level of allowable network access for the client machine based on the results; and instructing the access server to enforce the determined level of allowable network access; wherein determining the qualification procedures and standards of adequate protection comprises: determining a role for the client machine based on a prioritized set of attributes including two or more of MAC address of the client machine, subnet through which access is requested, IP address of the client machine, and network traffic information; updating, based on at least one outside source, information used to construct a plurality of policy rule sets providing different levels of network access requirements; and determining qualification procedures and standards of adequate protection associated with the determined role and the plurality of policy rule sets; wherein the method is performed by one or more computing devices.” (Claim 1). One of ordinary skill would find this limitation disclosed either expressly or inherently in the teachings of this reference and its incorporated disclosures taken as a whole, or in combination with the state of the art at the time of the alleged invention. To the extent this reference is not found to teach this element explicitly, implicitly, or inherently, the element would have been obvious to one of ordinary skill in the art based on this reference, common sense, ordinary creativity of one of ordinary skill in the art, and the state of the art. Additionally, it would have been obvious to combine this reference with one or more other prior art references identified in Defendant's Invalidity Contentions Cover Pleading, particularly, § IV (B). Rather than repeat those disclosures here, they are incorporated by reference into this chart.
[1F] determining, by the computing system, a compliance state of the	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation.

EXHIBIT E – CHENG

'038 Patent	Cheng
endpoint based on the status information and a plurality of compliance policies in the data store; and	Specifically, Cheng teaches that as the qualification authority, the access manager determines a compliance state of the endpoint (e.g., whether there is adequate protection on client machine) based on the status information (e.g., results of checks by the client agent) and a plurality of compliance policies in the data store (i.e., policy repository). For example, see the following passages and/or figures, as well as all related disclosures: Cheng: Cheng discloses that the "client agent applies the checks in the rule sets associated with the user's determined role, and "determines whether conditions defined by elements of the rule sets are true or false" (<i>determining . . . a compliance state of the endpoint based on the status information and a plurality of compliance policies</i>) the results are then "forwarded to the access manager via the access server at step 446" the "access manager" then "determine[s] whether the checks meet the standards of adequacy set by the rule sets" (<i>determining, by the computing system</i>). (12:33-38); (12:39-49). “The present invention relates to methods and devices for qualifying a client machine to access a network, based on policies governing required virus checking, operating system updates, worm, adware and/or malware protections.” (3:21-15). “A system administrator interacts with an access manager to establish user roles and select a set of policy rules and remediation procedures retrieved from the policy repository to be associated with the user roles. The access manager governs qualification of client machines for access to the network in accordance with the policy rules associated with the role of the user of the client machine.” (5:26-32). “A further aspect of the invention is an access server that serves as an intermediary between a client machine and the access manager, and enforces network access based on the qualification determinations made by the access manager. The client agent is another aspect of the invention. The client agent comprises software resident on a client machine and carries out certain checks, as

EXHIBIT E – CHENG

'038 Patent	Cheng
	indicated by the rule set, and reports the results via the access server to the access manager. The client agent may also receive automatic updates and patches via the access server. Particular aspects of the present invention are described in the claims, specification and drawings.” (5:33-44). “A client machine that fails to meet the standards of adequate protection may be redirected to remediation procedures that support efforts to bring the client machine into compliance with applicable policies.” (5:52-56). “Access manager 110 acts as a qualification authority. After successful authentication, access manager 110 may respond to a credentialed or authorized client, through an access server 120, 121 with procedures for making a qualification determination. In one embodiment, access manager 110 provides policy rule sets to be applied by the client agent software 142, 154 on client machines that have the client agent software installed.” (6:55-62). “Rules are typically defined to determine the posture of the client machine being assessed, including but not limited to, presence or absence of certain software, the runtime status of certain software, or whether a software module is up-to-date.” (8:30-34). “Checks are atomic posture evaluation elements typically implemented through registry checks (presence/absence of registry keys, values of keys, etc.), file attribute checks, application status checks, service status checks, etc.” (8:39-42). “Role-based access means that different user groups can be subject to various types of qualification procedures and various standards of adequate protection. Role-based access controls network access based on user, device and traffic attributes or characteristics. In addition to security, differentiated services can be provided to various user groups, as each defined role can be mapped to one more

EXHIBIT E – CHENG

'038 Patent	Cheng
	security or access policies that define authorization levels for that user or user group. Role-based access allows for highly granular control of user network access.” (9:50-59). “At step 410, a client attempts to connect to a network. For example, a user may access an access point on a wireless LAN with his laptop computer.” (10:64-66). “A user may enter user identification information as part of the request for access. For example, a user may enter a user identifier and a password, or use a biometric appliance. A secure web login page, or alternatively the clean agent software resident on client machines, may be used to present a login interface and obtain identification information from the user.” (11:4-10). “At step 415, information such as user identifier, client machine MAC address or other device identifier may be used to determine whether or not the user's client machine is on the clean list. If the client machine is on the clean list, it is exempt from qualification procedures. In this case, the user is given access to the network according to the user role that is determined in step 430, as shown by steps 432 and 465, discussed below. Although shown in FIG. 4, the use of a clean list is an optional feature, and is not required in all systems that qualify client machines to access a network. If there is no clean list, every client machine attempting to access the network must pass qualification procedures in order to access the network with every session.” (11:11-23). “The role may be determined from a number of attributes. For example, the MAC address of the client machine, the subnet through which access is requested, the IP address of the client machine and the user identifier may all be used to determine a role. In one embodiment, the MAC address is given higher priority than the user identifier, such that if a user's login identifier associates him with ‘Role B’, but the MAC address associates the client with ‘Role A’, ‘Role A’ may be used instead of Role B. Other priorities may be configured.” (11:39-48).

EXHIBIT E – CHENG

'038 Patent	Cheng
	“At step 444, the client agent applies the checks in the rule sets associated with the user's determined role, and determines whether conditions defined by elements of the rule sets are true or false. For example, the registry can be scanned for the latest virus definition files or for operating system vulnerabilities, according to various checks in the rule sets.” (12:33-38). “Any results from the checks are forwarded to the access manager via the access server at step 446. The rule sets may not indicate what results of applying the checks will result in qualification to access the network. Reporting the results of the checks may simply include reporting a set of true and false indications. Alternatively, rule sets could fully describe conditions necessary for qualification and the resident client agent software could report the sum evaluation of the checks. These results are evaluated by the access manager to determine whether the checks meet the standards of adequacy set by the rule sets, as indicated by step 448.” (12:39-49). “Results of the network-based scans are sent from the access server to the access manager. At step 460, the access manager determines whether the client machine meets the standards of adequate protection associated with the network-based scans. If the client machine meets these standards, then the client machine has met all standards of adequate protection, and the user is given his normal login role at step 485.” (13:43-49).

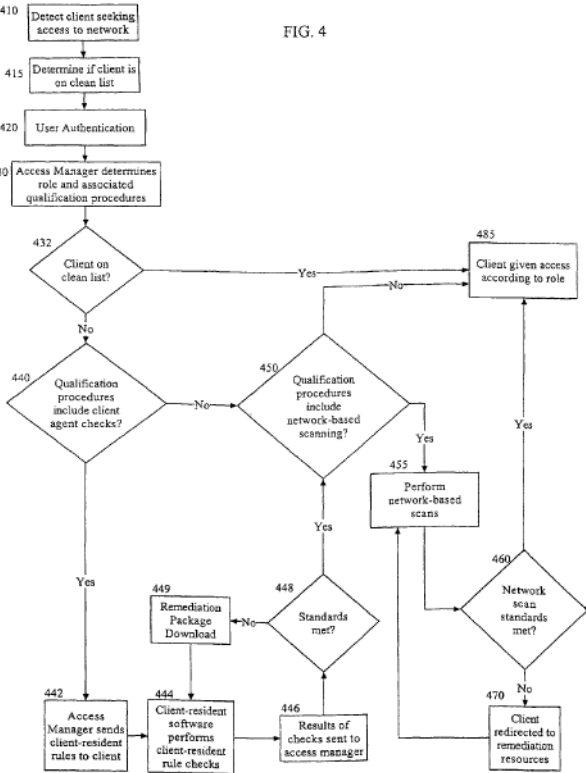
'038 Patent	Cheng
	FIG. 4  <pre> graph TD 410[410 Detect client seeking access to network] --> 415[415 Determine if client is on clean list] 415 --> 420[420 User Authentication] 420 --> 430[430 Access Manager determines role and associated qualification procedures] 430 --> 432{432 Client on clean list?} 432 -- Yes --> 485[485 Client given access according to role] 432 -- No --> 440{440 Qualification procedures include client agent checks?} 440 -- Yes --> 442[442 Access Manager sends client-resident rules to client] 442 --> 444[444 Client-resident software performs client-resident rule checks] 444 --> 446[446 Results of checks sent to access manager] 446 --> 448{448 Standards met?} 448 -- No --> 449[449 Remediation Package Download] 449 --> 444 448 -- Yes --> 455[455 Perform network-based scans] 455 --> 460{460 Network scan standards met?} 460 -- Yes --> 485 460 -- No --> 470[470 Client redirected to remediation resources] 440 -- No --> 450{450 Qualification procedures include network-based scanning?} 450 -- Yes --> 455 450 -- No --> 485 </pre> FIG. 4. “1. A method of qualifying a client machine to access a network, comprising the computer-implemented steps of: receiving a request for access from the client machine from an access server through which the client machine must first go to access the network, said request including user identification information; determining qualification procedures and standards of adequate protection for the client machine based on the user identification information;

EXHIBIT E – CHENG

'038 Patent	Cheng
	sending the determined qualification procedures to the access server, receiving from the access server results of applying the qualification procedures at the client machine; determining a level of allowable network access for the client machine based on the results; and instructing the access server to enforce the determined level of allowable network access; wherein determining the qualification procedures and standards of adequate protection comprises: determining a role for the client machine based on a prioritized set of attributes including two or more of MAC address of the client machine, subnet through which access is requested, IP address of the client machine, and network traffic information; updating, based on at least one outside source, information used to construct a plurality of policy rule sets providing different levels of network access requirements; and determining qualification procedures and standards of adequate protection associated with the determined role and the plurality of policy rule sets; wherein the method is performed by one or more computing devices.” (Claim 1). One of ordinary skill would find this limitation disclosed either expressly or inherently in the teachings of this reference and its incorporated disclosures taken as a whole, or in combination with the state of the art at the time of the alleged invention. To the extent this reference is not found to teach this element explicitly, implicitly, or inherently, the element would have been obvious to one of ordinary skill in the art based on this reference, common sense, ordinary creativity of one of ordinary skill in the art, and the state of the art. Additionally, it would have been obvious to combine this reference with one or more other prior art references identified in Defendant's Invalidity Contentions Cover Pleading, particularly, § IV (B). Rather than repeat those disclosures here, they are incorporated by reference into this chart.
[1G] initiating, by the computing system, based on the compliance state, an action identified in at least one rule in the data store,	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation.

EXHIBIT E – CHENG

'038 Patent	Cheng
wherein the action is carried out by a processor on the endpoint.	Specifically, Cheng teaches that, e.g., remediation action, such as implementing up-to-date virus checking options, as identified by a rule requiring the latest antivirus version be installed on the client machine, may be taken on the client machine based on the compliance state. For example, see the following passages and/or figures, as well as all related disclosures: Cheng: Cheng discloses that if it is determined that a "client machine does not meet the established standard, access manager 121 may notify the user of the determination" and that if the "client machine that fails to meet the standards of adequate protection" then it "may be redirected to remediation procedures" (<i>initiating, by the computing system, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by a processor on the endpoint</i>). (5:52-56); (12:50-54). "The remediation resources can assist an end user with updating and patching a machine according to policies set by an administrator. Unless the user fixes the problem, the user will not be allowed access to the network. In effect, administrators can also push patches and software updates to end client machines without user intervention, on either a scheduled or event basis, by requiring use of the remediation resources as a condition of network access. Users can no longer ignore patch update messages, and avoid complying with IT policies." (5:1-10). "In one embodiment, a policy repository stores 'policy rules' specified as combinations of conditions. The policy rules are updated regularly, such that the qualification procedures can check that the latest antivirus version has been installed on a client machine, etc. In one embodiment, the conditions generally include "checks." A check may be a test run by web-based scanning programs and/or a test that can be executed by software resident on a client machine. In this embodiment, the checks in the policy rules are used as the qualification procedures." (5:11-20).

EXHIBIT E – CHENG

'038 Patent	Cheng
	“The present invention relates to methods and devices for qualifying a client machine to access a network, based on policies defined by an administrator. In particular, when a client machine attempts to connect to a network, it must meet standards of adequate protection by applying various qualification procedures, such as checks performed by client agent software resident on a client machine. A client machine that fails to meet the standards of adequate protection may be redirected to remediation procedures that support efforts to bring the client machine into compliance with applicable policies.” (5:46-56). “Remediation resources 160 also are indicated in FIG. 1. A logical path 136 between the client machine 145 and remediation resources 160 indicates limited access to resources that may be provided to a client machine. The user can use the resources to fix detected problems on the client machine in order to meet the required standards of adequate protection. For example, the remediation resources may locally provide one or more up-to-date virus checking options (engine and definitions), or may provide links and limited access to outside resources such as virus checking vendor web sites. In one embodiment, remediation resources include remediation packages that are downloaded to the client agent software resident on client machines for automatic or user click-through execution. Remediation packages may include updated files or patches from anti-virus vendors, operating systems service packs, virus fix tools, etc.” (7:1-16). “Information provided by outside sources can be used to construct policy rule sets and remediation procedures. A policy rule set defines the tests that determine whether a client seeking access to the network has implemented particular protective measures. Policy rule sets further set standards for adequacy for the particular protective measures. For example, a rule set may set a standard of adequate protection for anti-virus protection, operating system update installation, worms, spyware, malware and/or adware. As additional protective measures are developed, it is anticipated that one of ordinary skill in the art will recognize how techniques disclosed herein can be adapted to include later developed protective measures. The standards of adequacy in policy rule sets are used to determine whether a client machine should be blocked from accessing the network.” (8:12-26).

EXHIBIT E – CHENG

'038 Patent	Cheng
	“If it is determined that the client machine does not meet the established standards, the access manager 121 may notify the user of the determination. In one embodiment, the user is placed in a "temporary" role such that access to the network is limited to the access configured for the temporary role.” (12:50-54). “If the qualification procedures do not require the client agent software at step 440, or if the client meets the standards established for the client agent qualification procedures at step 448, the process continues to step 450. If there are any network-based scans included in the qualification procedures, the process continues to step 455, where the access server performs the network-based scans of the client machine. If there are no network-based scans to apply, then the process continues to step 485, where the user is given his normal login role, with its associated privileges.” (13:33-42). “Results of the network-based scans are sent from the access server to the access manager. At step 460, the access manager determines whether the client machine meets the standards of adequate protection associated with the network-based scans. If the client machine meets these standards, then the client machine has met all standards of adequate protection, and the user is given his normal login role at step 485.” (13:43-49). “Alternatively or in addition, if the client agent software is installed on the client machine, the quarantine role can be configured to cause packages of fix tools and/or executables, such as anti-virus software updates, to be automatically downloaded to the quarantined machine.” (14:5-9). “FIG. 3 is a block diagram that illustrates a computer system 300 upon which an embodiment of the invention may be implemented.” (14:11-13).

'038 Patent	Cheng
	FIG. 4 <pre> graph TD 410[410 Detect client seeking access to network] --> 415[415 Determine if client is on clean list] 415 --> 420[420 User Authentication] 420 --> 430[430 Access Manager determines role and associated qualification procedures] 430 --> 432{432 Client on clean list?} 432 -- Yes --> 485[485 Client given access according to role] 432 -- No --> 440{440 Qualification procedures include client agent checks?} 440 -- Yes --> 442[442 Access Manager sends client-resident rules to client] 442 --> 444[444 Client-resident software performs client-resident rule checks] 444 --> 446[446 Results of checks sent to access manager] 446 --> 448{448 Standards met?} 448 -- No --> 449[449 Remediation Package Download] 448 -- Yes --> 450{450 Qualification procedures include network-based scanning?} 450 -- Yes --> 455[455 Perform network-based scans] 455 --> 460{460 Network scan standards met?} 460 -- No --> 470[470 Client redirected to remediation resources] 460 -- Yes --> 485 440 -- No --> 450 </pre> FIG. 4. “1. A method of qualifying a client machine to access a network, comprising the computer-implemented steps of:

EXHIBIT E – CHENG

'038 Patent	Cheng
	receiving a request for access from the client machine from an access server through which the client machine must first go to access the network, said request including user identification information; determining qualification procedures and standards of adequate protection for the client machine based on the user identification information; sending the determined qualification procedures to the access server, receiving from the access server results of applying the qualification procedures at the client machine; determining a level of allowable network access for the client machine based on the results; and instructing the access server to enforce the determined level of allowable network access; wherein determining the qualification procedures and standards of adequate protection comprises: determining a role for the client machine based on a prioritized set of attributes including two or more of MAC address of the client machine, subnet through which access is requested, IP address of the client machine, and network traffic information; updating, based on at least one outside source, information used to construct a plurality of policy rule sets providing different levels of network access requirements; and determining qualification procedures and standards of adequate protection associated with the determined role and the plurality of policy rule sets; wherein the method is performed by one or more computing devices.” (Claim 1). One of ordinary skill would find this limitation disclosed either expressly or inherently in the teachings of this reference and its incorporated disclosures taken as a whole, or in combination with the state of the art at the time of the alleged invention. To the extent this reference is not found to teach this element explicitly, implicitly, or inherently, the element would have been obvious to one of ordinary skill in the art based on this reference, common sense, ordinary creativity of one of ordinary skill in the art, and the state of the art. Additionally, it would have been obvious to combine this reference with one or more other prior art references identified in Defendant's Invalidity Contentions Cover Pleading, particularly, § IV (B). Rather than repeat those disclosures here, they are incorporated by reference into this chart.

EXHIBIT E – CHENG

'038 Patent	Cheng
2. The method of claim 1, wherein the action comprises controlling access of the endpoint to computing resources.	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. Specifically, Cheng teaches that access of the client machine to specific applications and resources (e.g., confidential financial databases) are controlled. For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim element [1G] which is incorporated by reference herein. <i>See also, e.g.:</i> Cheng: Cheng discloses "[t]he access server may be used to substantially prevent access of the rejected client to the network, pending remediation and successful qualification" (<i>the action comprises controlling access of the endpoint to computing resources</i>). (12:62-67). “Methods and devices for qualifying a client machine to access a network, based on policies governing required protective measures, such as virus checking and operating system updates, are disclosed. A client machine must pass various checks to qualify for access. A client machine may be redirected to remediation resources that support efforts to bring the client machine into compliance with applicable network access requirements. A policy repository is updated regularly by vendors of protective measures. An administrator establishes user roles that are mapped to policy rule sets retrieved from the policy repository. The policy rule sets govern qualification of client machines for access to the network in accordance with the roles of the users of the machines. An access server is an intermediary between a client machine and the access manager. A client agent runs on the client machine and carries out checks, and reports the results via the access server to the access manager.” (Abstract).

EXHIBIT E – CHENG

'038 Patent	Cheng
	“The techniques disclosed herein integrate with an enterprise's existing authentication authority to apply role-based policy enforcement upon login to the enterprise network. Role-based policy enforcement allows access to be restricted to only applications and resources determined to be necessary to the role of the user. A web-based administrator console is used to define role-based security policies for various classes of users, from guest users, such as contractors, to system administrators, or executives of a company. For example, roles may be established such that only users with sufficient “executive” privileges, such as a Chief Financial Officer, or other executives, are allowed to access confidential financial databases. As another example, a “guest” role may be established that allows a contractor or other guest access to only public information. Based on user identifier, MAC (Media Access Control) address and IP (Internet Protocol) address, the user's role and associated privileges are tied to the specific device used to access the network.” (3:31-48). “Access servers are used to enforce qualification determinations by exercising control over all packets coming from any client machine to the network.” (6:34-37). “Role-based access controls network access based on user, device and traffic attributes or characteristics. In addition to security, differentiated services can be provided to various user groups, as each defined role can be mapped to one more security or access policies that define authorization levels for that user or user group. Role-based access allows for highly granular control of user network access.” (9:52-59). “At step 430, a role is determined for the user. If the user is authenticated and authorized by the credentials authority, the access manager may then determine a role based on the user's identification, the type of machine the user is using, whether the machine is on the clean list, and optionally even network traffic information. If the client is not authenticated at step 420, the role assigned may be that of a "guest" user.” (11:32-38).

EXHIBIT E – CHENG

'038 Patent	Cheng
	“The access server may be used to substantially prevent access of the rejected client to the network, pending remediation and successful qualification. The access server may enforce navigation limits, time limits or both on a client pursuing remediation resources according to the temporary role. Access may be controlled by packet filtering.” (12:62-67). One of ordinary skill would find this limitation disclosed either expressly or inherently in the teachings of this reference and its incorporated disclosures taken as a whole, or in combination with the state of the art at the time of the alleged invention. To the extent this reference is not found to teach this element explicitly, implicitly, or inherently, the element would have been obvious to one of ordinary skill in the art based on this reference, common sense, ordinary creativity of one of ordinary skill in the art, and the state of the art. Additionally, it would have been obvious to combine this reference with one or more other prior art references identified in Defendant's Invalidity Contentions Cover Pleading, particularly, § IV (B). Rather than repeat those disclosures here, they are incorporated by reference into this chart.
3. The method of claim 1, wherein the user interface comprises a web page.	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. Specifically, Cheng teaches the use of a web-based application, accessible through any browser, to access and configure the access manager. For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim element [1A] which is incorporated by reference herein. <i>See also, e.g.:</i> Cheng:

EXHIBIT E – CHENG

'038 Patent	Cheng
	Cheng discloses that the "administrator console" is "a web-based application, accessible through any browser" (<i>the user interface comprises a web page</i>). (6:64-67). “The techniques disclosed herein integrate with an enterprise's existing authentication authority to apply role-based policy enforcement upon login to the enterprise network. Role-based policy enforcement allows access to be restricted to only applications and resources determined to be necessary to the role of the user. A web-based administrator console is used to define role-based security policies for various classes of users, from guest users, such as contractors, to system administrators, or executives of a company. For example, roles may be established such that only users with sufficient “executive” privileges, such as a Chief Financial Officer, or other executives, are allowed to access confidential financial databases. As another example, a “guest” role may be established that allows a contractor or other guest access to only public information. Based on user identifier, MAC (Media Access Control) address and IP (Internet Protocol) address, the user's role and associated privileges are tied to the specific device used to access the network.” (3:31-48). “A web-based administrator console is used to define role-based security policies for various classes of users, from guest users, such as contractors, to system administrators, or executives of a company.” (3:36-39). “Preferably, administrator console 112 is a web-based application, accessible through any browser. For example, the administrator console may be a Secure Sockets Layer (SSL)-enabled browser application. (6:64-67). One of ordinary skill would find this limitation disclosed either expressly or inherently in the teachings of this reference and its incorporated disclosures taken as a whole, or in combination with the state of the art at the time of the alleged invention. To the extent this reference is not found to teach this element explicitly, implicitly, or inherently, the element would have been obvious to one of ordinary skill in the art based on this reference, common sense, ordinary creativity of one of ordinary

EXHIBIT E – CHENG

'038 Patent	Cheng
	skill in the art, and the state of the art. Additionally, it would have been obvious to combine this reference with one or more other prior art references identified in Defendant's Invalidity Contentions Cover Pleading, particularly, § IV (B). Rather than repeat those disclosures here, they are incorporated by reference into this chart.
4. The method of claim 1, further comprising requesting, at the computing system, the status information on a periodic basis.	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. Specifically, Cheng teaches e.g., a policy server that regularly receives up-to-date information so that up-to-date status information can be requested on a periodic basis. For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim element [1E] which is incorporated by reference herein. <i>See also, e.g.:</i> Cheng: Cheng discloses a "client agent" that "carries out certain checks" and "reports the results via the access server to the access manager" (<i>requesting, at the computing system, the status information on a periodic basis</i>). (5:37-40). "In one embodiment, the access manager 110 may be comprised of multiple functional components. FIG. 2 illustrates one embodiment of an access manager that includes a policy server 220 and a rules manager 230. Policy server 220 and rules manager 230 may run on separate servers, or separate server clusters, or they may run together on the same server or server cluster. Although only a single rules manager is shown in FIG. 2, a policy server may provide policy rule sets to many rules managers located in many different networks." (7:23-31).

EXHIBIT E – CHENG

'038 Patent	Cheng
	“The policy server 220 regularly receives up-to-date information from outside sources 240. The policy server may pull the information on a periodic or event driven basis. Optionally, outside sources could notify a policy server of available updates. Alternatively, a system could be configured such that outside sources 240 automatically push updates to the policy server 220 when updates occur, or on a configured periodic basis. Additional outside sources can be added at any time as new protective measures become available.” (7:62-8:3). “In addition, the policy server 220 may obtain qualitative information from the virus checking vendors regarding the significance (e.g., high, medium or low) of versions of various protective measures, and use that qualitative information to establish different standards of adequate protection for different policy rule sets.” (8:62-67). “The access server may enforce navigation limits, time limits or both on a client pursuing remediation resources according to the temporary role.” (12:64-67). One of ordinary skill would find this limitation disclosed either expressly or inherently in the teachings of this reference and its incorporated disclosures taken as a whole, or in combination with the state of the art at the time of the alleged invention. To the extent this reference is not found to teach this element explicitly, implicitly, or inherently, the element would have been obvious to one of ordinary skill in the art based on this reference, common sense, ordinary creativity of one of ordinary skill in the art, and the state of the art. Additionally, it would have been obvious to combine this reference with one or more other prior art references identified in Defendant's Invalidity Contentions Cover Pleading, particularly, § IV (B). Rather than repeat those disclosures here, they are incorporated by reference into this chart.
5. The method of claim 1, wherein the endpoint comprises a mobile device.	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation.

EXHIBIT E – CHENG

'038 Patent	Cheng
	Specifically, Cheng teaches that the client machine can be, e.g., any IP-enabled end station device that can access a network, including mobile devices. For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re preamble [1P], claim element [1A] which are incorporated by reference herein. <i>See also, e.g.:</i> Cheng: Cheng discloses, generally, that "mobile devices" are used to connect to networks (<i>the endpoint comprises a mobile device</i>). (1:45-49); (2:34-38). “Connection of mobile devices to networks presents even greater challenges for protecting networks, as the growth in access points has resulted in an increase in points of vulnerability in the network, and has allowed viruses to spread at ever faster rates.” (1:45-49). “Mobile devices attach to networks over which IT has no control. It is much more challenging to protect a network against software that is loaded and active when a mobile device gains access to the network than to protect a desktop from accidentally downloading a virus over controlled network channels.” (1:56-61). “One approach to protecting a network has been to enforce the presence of a particular virus checker on machines seeking Internet access through controlled network channels. For instance, SonicWALL™ firewalls can be configured to enforce installation of an edition of McAfee's virus checking software. However, the firewall's enforcement mechanism is limited to blocking Internet access, as firewalls are conceptually placed on the perimeter of a network, facing the Internet. A firewall can block the spread of viruses between different networks, but not within the network itself.

EXHIBIT E – CHENG

'038 Patent	Cheng
	The firewall's checking mechanism is only invoked when a user attempts to reach the Internet through the firewall, and it only checks for an active virus scanning program. A mobile device that joins the network will have free access to core network resources without necessarily invoking the firewall's checking mechanism.” (1:62-2:10). “Based on the foregoing, known techniques for managing the security of IP connected devices and software are inadequate, especially for mobile users that remotely access a network, and there is a need for alternative techniques for protecting a network.” (2:34-38). One of ordinary skill would find this limitation disclosed either expressly or inherently in the teachings of this reference and its incorporated disclosures taken as a whole, or in combination with the state of the art at the time of the alleged invention. To the extent this reference is not found to teach this element explicitly, implicitly, or inherently, the element would have been obvious to one of ordinary skill in the art based on this reference, common sense, ordinary creativity of one of ordinary skill in the art, and the state of the art. Additionally, it would have been obvious to combine this reference with one or more other prior art references identified in Defendant's Invalidity Contentions Cover Pleading, particularly, § IV (B). Rather than repeat those disclosures here, they are incorporated by reference into this chart.
6. The method of claim 1, wherein the one or more software agents comprise at least one service provided by the operating system of the endpoint.	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. Specifically, Cheng teaches that the client agent software is installed on the client machine and can perform services, such as registry, process, application and service checks, which are provided by the operating system of the client machine. For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim 1 which is incorporated by reference herein.

EXHIBIT E – CHENG

'038 Patent	Cheng
	<i>See also, e.g.:</i> Cheng: Cheng discloses that once the "client agent" is installed on the "client machine" the "client agent" then "perform[s] registry, process, application and service checks on the client machine" (<i>the one or more software agents comprise at least one service provided by the operating system of the endpoint</i>). (6:5-12). “A client machine 141, 153 may include optional client agent software 142, 154 resident on the client machine. Client agent software 142, 154, is not required, as shown by client machines 143, 145, 151, 155, 157. Not shown are various client resources available on the client machines. In general, client agent software resident on client machines provides local-machine agent-based vulnerability assessment and remediation. Once the client agent is downloaded and installed on a client machine, it can perform registry, process, application and service checks on the client machine. The results of these checks can be used to detect antivirus software installation, status and virus definition states. The client agent software 142,154 typically runs as a service, or alternatively it could be activated by a client that wants to access the network.” (5:65-6:12). “A policy rule set may include rules for interrogating a device attempting to access the network through optional client agent software resident on client machines. These policy rules may contain Boolean expressions of individual checks. Checks are atomic posture evaluation elements typically implemented through registry checks (presence/absence of registry keys, values of keys, etc.), file attribute checks, application status checks, service status checks, etc. Checks are combined using Boolean operators (including but not limited to AND, OR, NOT, EQUALS, LATER THAN, NEWER THAN, CONTAINS, SUBSTRING OF, EXISTS, DOES NOT EXIST, IS DEFAULT VALUE, etc.) to form a policy rule.” (8:35-47).

EXHIBIT E – CHENG

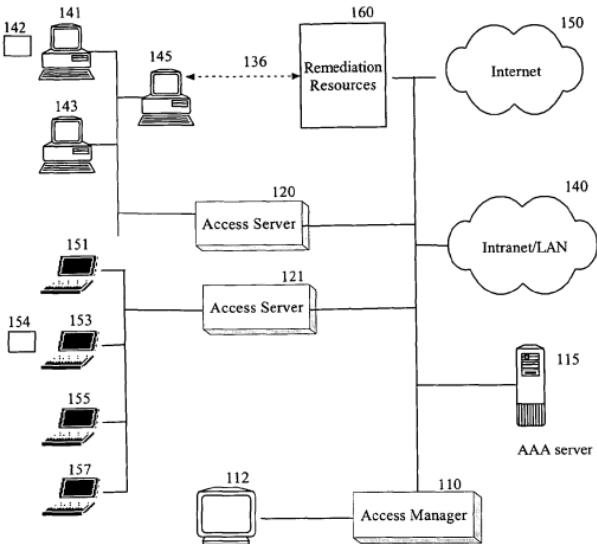
'038 Patent	Cheng
	“An application or service running check may determine whether an application or service is currently running on the client or an associated device.” (9:16-18). “The client agent rules are those that include checks that need to be performed by the software resident on the client machine due to security measures typically implemented by clients or operating systems. The client agent software on the client machine is invoked to perform the checks. In this sense, invoking may mean communicating with, as the resident software may be running as a service and may have identified the client seeking access.” (12:5-12).  FIG. 1

EXHIBIT E – CHENG

'038 Patent	Cheng
	FIG. 1. One of ordinary skill would find this limitation disclosed either expressly or inherently in the teachings of this reference and its incorporated disclosures taken as a whole, or in combination with the state of the art at the time of the alleged invention. To the extent this reference is not found to teach this element explicitly, implicitly, or inherently, the element would have been obvious to one of ordinary skill in the art based on this reference, common sense, ordinary creativity of one of ordinary skill in the art, and the state of the art. Additionally, it would have been obvious to combine this reference with one or more other prior art references identified in Defendant's Invalidity Contentions Cover Pleading, particularly, § IV (B). Rather than repeat those disclosures here, they are incorporated by reference into this chart.
7. The method of claim 1, wherein the one or more software agents comprise at least one application running on the endpoint.	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. Specifically, Cheng teaches that the client agent software is an application installed and running on the client machine. For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim element [1D] which is incorporated by reference herein. <i>See also, e.g.:</i> Cheng: Cheng discloses that in an internet example, a "downloaded application provides for automated provisioning of phones in packet voice networks as described herein" (<i>the one or more software agents comprise at least one application running on the endpoint</i>). (15:61-67).

EXHIBIT E – CHENG

'038 Patent	Cheng
	“A file attribute check may test the existence, size, date stamp, location or version of a particular file. An application or service running check may determine whether an application or service is currently running on the client or an associated device.” (9:13-17). “In the Internet example, a server 330 might transmit a requested code for an application program through Internet 328, ISP 326, local network 322 and communication interface 318. In accordance with the invention, one such downloaded application provides for automated provisioning of phones in packet voice networks as described herein.” (15:61-67). One of ordinary skill would find this limitation disclosed either expressly or inherently in the teachings of this reference and its incorporated disclosures taken as a whole, or in combination with the state of the art at the time of the alleged invention. To the extent this reference is not found to teach this element explicitly, implicitly, or inherently, the element would have been obvious to one of ordinary skill in the art based on this reference, common sense, ordinary creativity of one of ordinary skill in the art, and the state of the art. Additionally, it would have been obvious to combine this reference with one or more other prior art references identified in Defendant's Invalidity Contentions Cover Pleading, particularly, § IV (B). Rather than repeat those disclosures here, they are incorporated by reference into this chart.
8. The method of claim 1, wherein the conditions comprise at least one hardware condition.	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. Specifically, Cheng teaches the detection of, e.g., a MAC address of the client machine, to determine network access for the client machine. For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim element [1C] which is incorporated by reference herein.

EXHIBIT E – CHENG

'038 Patent	Cheng
	<i>See also, e.g.:</i> Cheng: Cheng discloses that “the user’s role and associated privileges” may be based on the MAC (Media Access Control) address“(the conditions comprise at least one hardware condition). (3:45-48). “Based on user identifier, MAC (Media Access Control) address and IP (Internet Protocol) address, the user's role and associated privileges are tied to the specific device used to access the network.” (3:45-48). “The role may be determined from a number of attributes. For example, the MAC address of the client machine, the subnet through which access is requested, the IP address of the client machine and the user identifier may all be used to determine a role. In one embodiment, the MAC address is given higher priority then the user identifier, such that if a user's login identifier associates him with ‘Role B’, but the MAC address associates the client with ‘Role A’, ‘Role A’ may be used instead of Role B. Other priorities may be configured.” (11:39-48). One of ordinary skill would find this limitation disclosed either expressly or inherently in the teachings of this reference and its incorporated disclosures taken as a whole, or in combination with the state of the art at the time of the alleged invention. To the extent this reference is not found to teach this element explicitly, implicitly, or inherently, the element would have been obvious to one of ordinary skill in the art based on this reference, common sense, ordinary creativity of one of ordinary skill in the art, and the state of the art. Additionally, it would have been obvious to combine this reference with one or more other prior art references identified in Defendant's Invalidity Contentions Cover Pleading, particularly, § IV (B). Rather than repeat those disclosures here, they are incorporated by reference into this chart.
9. The method of claim 1, wherein the conditions	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation.

EXHIBIT E – CHENG

'038 Patent	Cheng
comprise at least one software condition.	Specifically, Cheng teaches, e.g., detecting spyware, anti-virus software version, versions of virus definition files, and operating system update version information for determining network access for the client machine. For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim element [1C] which is incorporated by reference herein. <i>See also, e.g.:</i> Cheng: Cheng discloses that the "checks" include "registry checks (presence/absence of registry keys, values of keys, etc.), file attribute checks, application status checks, service status checks, etc." (<i>the conditions comprise at least one software condition</i>). (8:39-42). “Another type of qualification procedure is a device-based interrogation test. For this type of test, a client agent program is resident on a user's machine and used to execute the test. For example, the client agent program can scan the machine's registry for the latest virus definition files or operating system vulnerabilities. Network-based probes may not be possible on some machines due to security measures implemented by the client (such as a firewall) and/or its operating system. Device-based interrogation tests used to qualify a client machine may perform checks not possible with network-based scanning, such as detecting spyware, anti-virus software version, dates and/or versions of virus definition files, operating system update version information, etc., on the client machine.” (3:64-4:10). “The client agent comprises software resident on a client machine and carries out certain checks, as indicated by the rule set, and reports the results via the access server to the access manager.” (5:37-40)

EXHIBIT E – CHENG

'038 Patent	Cheng
	“In particular, when a client machine attempts to connect to a network, it must meet standards of adequate protection by applying various qualification procedures, such as checks performed by client agent software resident on a client machine.” (5:48-52). “Once the client agent is downloaded and installed on a client machine, it can perform registry, process, application and service checks on the client machine. The results of these checks can be used to detect antivirus software installation, status and virus definition states.” (6:5-9). “Rules are typically defined to determine the posture of the client machine being assessed, including but not limited to, presence or absence of certain software, the runtime status of certain software, or whether a software module is up-to-date.” (8:30-34). “Checks are atomic posture evaluation elements typically implemented through registry checks (presence/absence of registry keys, values of keys, etc.), file attribute checks, application status checks, service status checks, etc.” (8:39-42). One of ordinary skill would find this limitation disclosed either expressly or inherently in the teachings of this reference and its incorporated disclosures taken as a whole, or in combination with the state of the art at the time of the alleged invention. To the extent this reference is not found to teach this element explicitly, implicitly, or inherently, the element would have been obvious to one of ordinary skill in the art based on this reference, common sense, ordinary creativity of one of ordinary skill in the art, and the state of the art. Additionally, it would have been obvious to combine this reference with one or more other prior art references identified in Defendant's Invalidity Contentions Cover Pleading, particularly, § IV (B). Rather than repeat those disclosures here, they are incorporated by reference into this chart.

EXHIBIT E – CHENG

'038 Patent	Cheng
10. The method of claim 1, wherein the computing system comprises a plurality of servers.	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. Specifically, Cheng teaches that a plurality of servers, e.g., a policy server, an access server, credentials authority server, etc., is part of the computing system. For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim element [1A] which is incorporated by reference herein. <i>See also, e.g.:</i> Cheng: Cheng discloses that "client machines may have wired or wireless connections to access servers 120, 121". The network in Cheng also includes "Policy server 220 and rules manager 230 " which may run on the same or separate servers (<i>the computing system comprises a plurality of servers</i>). (6:13-15); (7:26-29). “A further aspect of the invention is an access server that serves as an intermediary between a client machine and the access manager, and enforces network access based on the qualification determinations made by the access manager. The client agent is another aspect of the invention. The client agent comprises software resident on a client machine and carries out certain checks, as indicated by the rule set, and reports the results via the access server to the access manager. The client agent may also receive automatic updates and patches via the access server. Particular aspects of the present invention are described in the claims, specification and drawings.” (5:33-44). “Client machines may have wired or wireless connections to access servers 120, 121. More or fewer access servers may be deployed in any given configuration.” (6:13-15).

EXHIBIT E – CHENG

'038 Patent	Cheng
	“Access servers can be deployed at the edge of a network, as shown in FIG. 1, or they may be deployed centrally.” (6:25-26). “A credentials authority server, such as AAA (Authentication, Authorization and Accounting) server 115, may be accessed through the access servers 120, 121 in response to an initial client request for access. The AAA server may comprise any server that handles user requests for access, and provides authentication, authorization and accounting services for an enterprise. One standard of communication that may be used by the AAA server is the Remote Authentication Dial-In User Service (RADIUS), although others such as TACACS+, are known to those skilled in the art and can be used. Although an AAA server is specifically shown in FIG. 1, any type of credentials authority that can authenticate and authorize users can be used. In addition, multiple credentials authority servers may be used. In one embodiment, a separate credentials authority server is not used, and the access manager 110 performs the authentication and authorization function.” (6:38-54). “Policy server 220 and rules manager 230 may run on separate servers, or separate server clusters, or they may run together on the same server or server cluster.” (7:26-29).

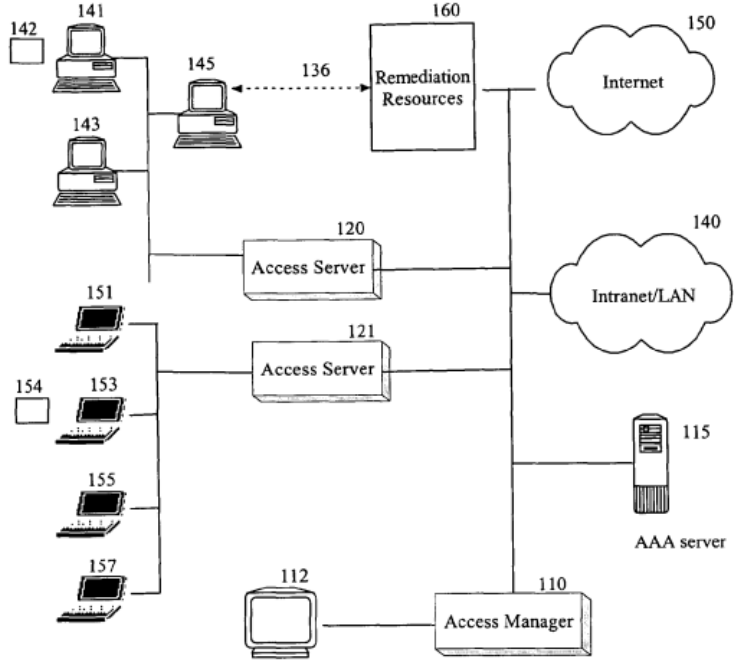
'038 Patent	Cheng
	 The diagram illustrates a network architecture. On the left, a group of client devices (141, 143, 151, 153, 155, 157) and a storage device (142) are connected to a central network. A dashed arrow (145) points from device 141 to a Remediation Resources block (160). A dashed arrow (136) points from the Remediation Resources block (160) to the Internet cloud (150). The central network consists of two Access Servers (120 and 121) and an Access Manager (110). The Access Manager (110) is connected to a monitor (112). The Access Servers (120 and 121) are connected to the Internet cloud (150) and the Intranet/LAN cloud (140). A AAA server (115) is also connected to the central network. The Remediation Resources block (160) is connected to the Internet cloud (150). FIG. 1 FIG. 1. One of ordinary skill would find this limitation disclosed either expressly or inherently in the teachings of this reference and its incorporated disclosures taken as a whole, or in combination with the state of the art at the time of the alleged invention. To the extent this reference is not found to teach this element explicitly, implicitly, or inherently, the element would have been obvious to one of ordinary skill in the art based on this reference, common sense, ordinary creativity of one of ordinary

EXHIBIT E – CHENG

'038 Patent	Cheng
	skill in the art, and the state of the art. Additionally, it would have been obvious to combine this reference with one or more other prior art references identified in Defendant's Invalidity Contentions Cover Pleading, particularly, § IV (B). Rather than repeat those disclosures here, they are incorporated by reference into this chart.
11. The method of claim 1, wherein the plurality of policies includes at least one policy that includes the at least one rule that identifies the action.	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. Specifically, Cheng teaches that, e.g., a policy requiring the latest antivirus version be installed on the client machine may include remediation action such as implementing up-to-date virus checking options. For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim elements [1A]-[1C], and [1G] which are incorporated by reference herein. <i>See also, e.g.:</i> Cheng: Cheng discloses that the of redirecting to "remediation procedures that support efforts to bring the client machine into compliance" (<i>identifies the action</i>) is based on "policies" (<i>the plurality of policies</i>) and that a "policy rule set is a collection of policy rules" (<i>at least one policy that includes the at least one rule</i>). (5:52-56); (8:27-34). “A client machine 141, 153 may include optional client agent software 142, 154 resident on the client machine. Client agent software 142, 154, is not required, as shown by client machines 143, 145, 151, 155, 157. Not shown are various client resources available on the client machines. In general, client agent software resident on client machines provides local-machine agent-based vulnerability assessment and remediation. Once the client agent is downloaded and installed on a client machine, it can perform registry, process, application and service checks on the client machine. The results of

EXHIBIT E – CHENG

'038 Patent	Cheng
	these checks can be used to detect antivirus software installation, status and virus definition states.” (5:65-6:9). “A policy rule set may include rules for interrogating a device attempting to access the network through optional client agent software resident on client machines. These policy rules may contain Boolean expressions of individual checks. Checks are atomic posture evaluation elements typically implemented through registry checks (presence/absence of registry keys, values of keys, etc.), file attribute checks, application status checks, service status checks, etc.” (8:35-42). “Rule sets may be constructed to provide different levels of network access requirements by including rules that have different qualification procedures, and/or including rules that have different standards of adequate protection.” (8:56-59). “The rules manager 230 receives policy rule sets from the policy server 220. The policy server may respond to electronic requests for the updated rule sets from the rules managers.” (9:24-27). One of ordinary skill would find this limitation disclosed either expressly or inherently in the teachings of this reference and its incorporated disclosures taken as a whole, or in combination with the state of the art at the time of the alleged invention. To the extent this reference is not found to teach this element explicitly, implicitly, or inherently, the element would have been obvious to one of ordinary skill in the art based on this reference, common sense, ordinary creativity of one of ordinary skill in the art, and the state of the art. Additionally, it would have been obvious to combine this reference with one or more other prior art references identified in Defendant's Invalidity Contentions Cover Pleading, particularly, § IV (B). Rather than repeat those disclosures here, they are incorporated by reference into this chart.
[12P] A non-transitory computer readable medium	To the extent the preamble is limiting, Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation.

EXHIBIT E – CHENG

'038 Patent	Cheng
containing computer instructions for controlling the operation of an endpoint, comprising:	Specifically, Cheng teaches a non-transitory computer readable medium containing computer instructions for controlling (e.g., qualifying) the operation of an endpoint (e.g., a client machine to access a network). For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim preamble [1P] which is incorporated by reference herein. <i>See also, e.g.:</i> Cheng: Cheng discloses "instructions may be read into main memory 306 from another computer-readable medium" and that "computer-readable medium" is a medium that provides instructions to the processor (<i>A non-transitory computer readable medium containing computer instructions for</i>), Cheng also discloses "access servers are used to enforce qualification determinations by exercising control over all packets coming from any client machine to the network (<i>controlling the operation of an endpoint</i>). (6:34-37); (14:48-53). “The invention is related to the use of computer system 300 for qualifying a client to access a network. According to one embodiment of the invention, qualification methods are provided by computer system 300 in response to processor 304 executing one or more sequences of one or more instructions contained in main memory 306. Such instructions may be read into main memory 306 from another computer-readable medium, such as storage device 310. Execution of the sequences of instructions contained in main memory 306 causes processor 304 to perform the process steps described herein. In alternative embodiments, hard-wired circuitry may be used in place of or in combination with software instructions to implement the invention. Thus, embodiments of the invention are not limited to any specific combination of hardware circuitry and software.” (14:43-57).

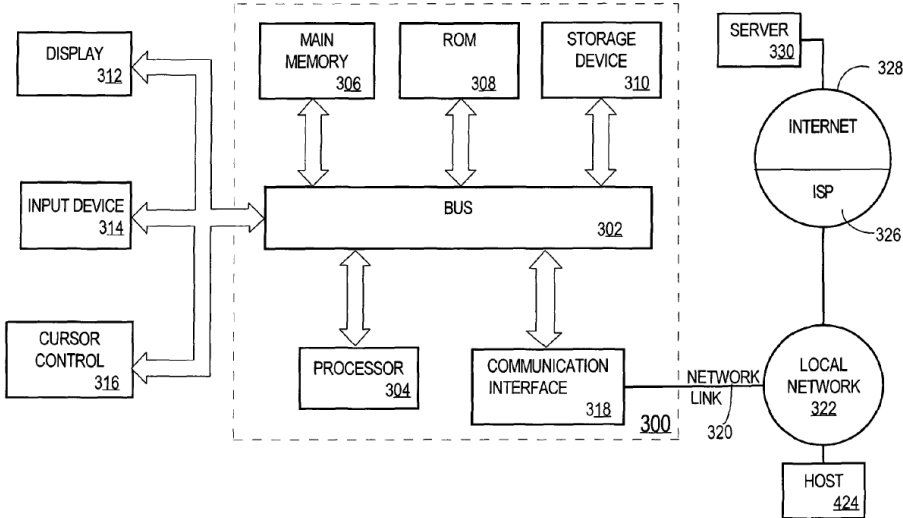
'038 Patent	Cheng
	“The term "computer-readable medium" as used herein refers to any medium that participates in providing instructions to processor 304 for execution.” (14:58-60). FIG. 3  FIG. 3. “Various forms of computer readable media may be involved in carrying one or more sequences of one or more instructions to processor 404 for execution.” (15:12-14). “17. A non-transitory computer-readable storage medium storing one or more sequences of instructions which when executed, cause one or more processors to perform” (Claim 17).

EXHIBIT E – CHENG

'038 Patent	Cheng
	One of ordinary skill would find this limitation disclosed either expressly or inherently in the teachings of this reference and its incorporated disclosures taken as a whole, or in combination with the state of the art at the time of the alleged invention. To the extent this reference is not found to teach this element explicitly, implicitly, or inherently, the element would have been obvious to one of ordinary skill in the art based on this reference, common sense, ordinary creativity of one of ordinary skill in the art, and the state of the art. Additionally, it would have been obvious to combine this reference with one or more other prior art references identified in Defendant's Invalidity Contentions Cover Pleading, particularly, § IV (B). Rather than repeat those disclosures here, they are incorporated by reference into this chart.
[12A] providing a user interface, at a computing system remote from the end point, configured to allow configuration of a plurality of policies;	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim element [1A] which is incorporated by reference herein.
[12B] maintaining the plurality of policies in a data store on the computing system;	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim element [1B] which is incorporated by reference herein.
[12C] identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to monitor;	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim element [1C] which is incorporated by reference herein.

EXHIBIT E – CHENG

'038 Patent	Cheng
[12D] configuring one or more software agents on the endpoint to monitor the plurality of operating conditions;	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim element [1D] which is incorporated by reference herein.
[12E] receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint gathered by the one or more software agents;	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim element [1E] which is incorporated by reference herein.
[12F] determining, by the computing system, a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store; and	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim element [1F] which is incorporated by reference herein.
[12G] initiating, by the computing system, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim element [1G] which is incorporated by reference herein.

EXHIBIT E – CHENG

'038 Patent	Cheng
out by a processor on the endpoint.	
13. The computer readable medium of claim 12, wherein the action comprises controlling access of the endpoint to computing resources.	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim 2 which is incorporated by reference herein.
14. The computer readable medium of claim 12, wherein the user interface comprises a web page.	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim 3 which is incorporated by reference herein.
15. The computer readable medium of claim 12, further comprising requesting, at the computing system, the status information on a periodic basis.	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim 4 which is incorporated by reference herein.
16. The computer readable medium of claim 12, wherein the endpoint comprises a mobile device.	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim 5 which is incorporated by reference herein.

EXHIBIT E – CHENG

'038 Patent	Cheng
17. The computer readable medium of claim 12, wherein the one or more software agents comprise at least one service provided by the operating system of the endpoint.	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim 6 which is incorporated by reference herein.
18. The computer readable medium of claim 12, wherein the one or more software agents comprise at least one application running on the endpoint.	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim 7 which is incorporated by reference herein.
19. The computer readable medium of claim 12, wherein the conditions comprise at least one hardware condition.	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim 8 which is incorporated by reference herein.
20. The computer readable medium of claim 12, wherein the conditions comprise at least one software condition.	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim 9 which is incorporated by reference herein.
21. The computer readable medium of claim 12,	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation.

EXHIBIT E – CHENG

'038 Patent	Cheng
wherein the computing system comprises a plurality of servers.	For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim 10 which is incorporated by reference herein.
22. The computer readable medium of claim 12, wherein the plurality of policies includes at least one policy that includes the at least one rule that identifies the action.	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim 11 which is incorporated by reference herein.
[23P] A system for controlling the operation of an endpoint, comprising:	To the extent the preamble is limiting, Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. Specifically, Cheng teaches a system for controlling (e.g., qualifying) the operation of an endpoint (e.g., a client machine to access a network). For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim preambles [1P], [12P] which are incorporated by reference herein. <i>See also, e.g.:</i> Cheng: Cheng discloses a "computer system 300 for qualifying a client to access a network" and that the invention of Cheng may be a "system for qualifying a client machine to access a network" (<i>A system for controlling the operation of an endpoint</i>). (14:43-48); Claim 14.

EXHIBIT E – CHENG

'038 Patent	Cheng
	“Although shown in FIG. 4, the use of a clean list is an optional feature, and is not required in all systems that qualify client machines to access a network.” (11:18-20). “FIG. 3 is a block diagram that illustrates a computer system 300 upon which an embodiment of the invention may be implemented.” (14:11-13). “The invention is related to the use of computer system 300 for qualifying a client to access a network. According to one embodiment of the invention, qualification methods are provided by computer system 300 in response to processor 304 executing one or more sequences of one or more instructions contained in main memory 306.” (14:43-48). “The present invention may be practiced as a method or device adapted to practice the method. The same method can be viewed from the perspective of a system, a policy server, a rules manager or server, an access server that enforces a qualification process, or software resident on a client seeking to gain access to the network.” (16:14-19). “14. A system for qualifying a client machine to access a network, comprising: one or more processors; a computer-readable storage medium storing one or more sequences of instructions, which when executed cause the one or more processors to provide” (Claim 14). One of ordinary skill would find this limitation disclosed either expressly or inherently in the teachings of this reference and its incorporated disclosures taken as a whole, or in combination with the state of the art at the time of the alleged invention. To the extent this reference is not found to teach this element explicitly, implicitly, or inherently, the element would have been obvious to one of ordinary skill in the art based on this reference, common sense, ordinary creativity of one of ordinary

EXHIBIT E – CHENG

'038 Patent	Cheng
	skill in the art, and the state of the art. Additionally, it would have been obvious to combine this reference with one or more other prior art references identified in Defendant's Invalidity Contentions Cover Pleading, particularly, § IV (B). Rather than repeat those disclosures here, they are incorporated by reference into this chart.
[23A] a user interface, provided by a computing system remote from the end point, configured to allow configuration of a plurality of policies;	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim element [1A] which is incorporated by reference herein.
[23B] a data store, at the computing system, that contains the plurality of policies;	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim element [1B] which is incorporated by reference herein.
[23C] one or more software agents on the endpoint configured to monitor a plurality of operating conditions identified in the plurality of policies; and	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim elements [1C] and [1D] which are incorporated by reference herein.
[23D] one or more hardware processors at the computing system configured to:	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. Specifically, Cheng teaches a user interface (e.g., an access manager using one or more hardware processors) at a computing system remote from the end point (e.g., client machine) and configured to

EXHIBIT E – CHENG

'038 Patent	Cheng
	allow configuration of a plurality of policies (e.g., allowing the access manager to configure policy rule sets). For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim element [1A] which is incorporated by reference herein. <i>See also, e.g.:</i> Cheng: Cheng discloses a "processor" (<i>one or more hardware processors</i>) that is included in a "computer system" (<i>at the computing system</i>). (14:11-16). “FIG. 3 is a block diagram that illustrates a computer system 300 upon which an embodiment of the invention may be implemented. Computer system 300 includes a bus 302 or other communication mechanism for communicating information, and a processor 304 coupled with bus 302 for processing information.” (14:11-16). “The invention is related to the use of computer system 300 for qualifying a client to access a network. According to one embodiment of the invention, qualification methods are provided by computer system 300 in response to processor 304 executing one or more sequences of one or more instructions contained in main memory 306.” (14:43-48). “Execution of the sequences of instructions contained in main memory 306 causes processor 304 to perform the process steps described herein. In alternative embodiments, hard-wired circuitry may be used in place of or in combination with software instructions to implement the invention. Thus, embodiments of the invention are not limited to any specific combination of hardware circuitry and software.”

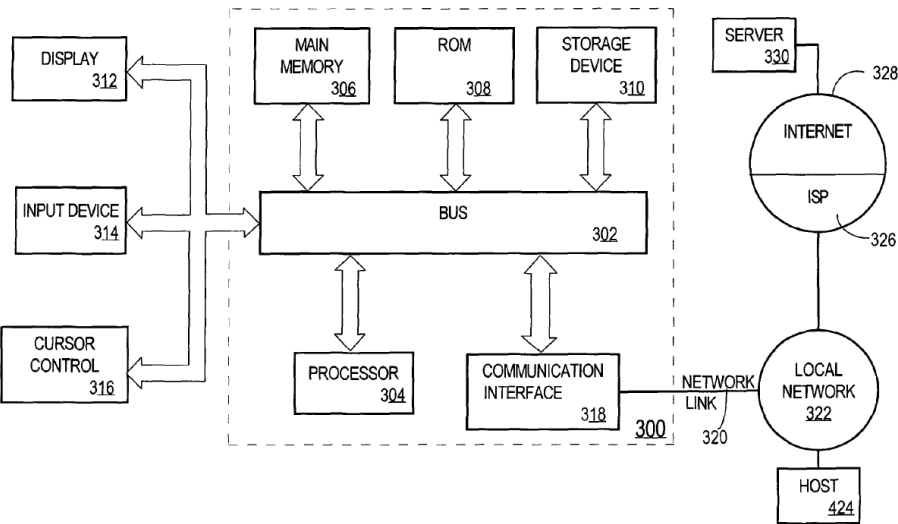
'038 Patent	Cheng
	(14:50-57). FIG. 3  FIG. 3. “14. A system for qualifying a client machine to access a network, comprising: one or more processors; a computer-readable storage medium storing one or more sequences of instructions, which when executed cause the one or more processors to provide...) Claim 14. One of ordinary skill would find this limitation disclosed either expressly or inherently in the teachings of this reference and its incorporated disclosures taken as a whole, or in combination with the state of the art at the time of the alleged invention. To the extent this reference is not found to teach this element explicitly, implicitly, or inherently, the element would have been obvious to one of ordinary skill in the art based on this reference, common sense, ordinary creativity of one of ordinary

EXHIBIT E – CHENG

'038 Patent	Cheng
	skill in the art, and the state of the art. Additionally, it would have been obvious to combine this reference with one or more other prior art references identified in Defendant's Invalidity Contentions Cover Pleading, particularly, § IV (B). Rather than repeat those disclosures here, they are incorporated by reference into this chart.
[23E] receive, across a network, status information about the plurality of operating conditions on the endpoint gathered by the one or more software agents,	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim element [1E] which is incorporated by reference herein.
[23F] determine a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store, and	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim element [1F] which is incorporated by reference herein.
[23G] initiate, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by the hardware processor on the endpoint.	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim elements [1G] and [23D] which are incorporated by reference herein.
24. The system of claim 23, wherein the action comprises controlling	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation.

EXHIBIT E – CHENG

'038 Patent	Cheng
access of the endpoint to computing resources.	For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim 2 which is incorporated by reference herein.
25. The system of claim 23, wherein the user interface comprises a web page.	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim 3 which is incorporated by reference herein.
26. The system of claim 23, wherein the one or more processors are further configured to request the status information from the endpoint on a periodic basis.	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. Specifically, Cheng teaches e.g., a policy server that regularly receives up-to-date information so that up-to-date status information can be requested on a periodic basis. For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim element [23D] and claim 4 which are incorporated by reference herein. <i>See also, e.g.:</i> Cheng: Cheng discloses a "client agent" that "carries out certain checks" and "reports the results via the access server to the access manager" (<i>wherein the one or more processors are further configured to request the status information from the endpoint on a periodic basis</i>). (5:37-40). “The policy rules are updated regularly, such that the qualification procedures can check that the latest antivirus version has been installed on a client machine, etc. In one embodiment, the conditions

EXHIBIT E – CHENG

'038 Patent	Cheng
	generally include "checks." A check may be a test run by web-based scanning programs and/or a test that can be executed by software resident on a client machine. In this embodiment, the checks in the policy rules are used as the qualification procedures.” (5:12-20) One of ordinary skill would find this limitation disclosed either expressly or inherently in the teachings of this reference and its incorporated disclosures taken as a whole, or in combination with the state of the art at the time of the alleged invention. To the extent this reference is not found to teach this element explicitly, implicitly, or inherently, the element would have been obvious to one of ordinary skill in the art based on this reference, common sense, ordinary creativity of one of ordinary skill in the art, and the state of the art. Additionally, it would have been obvious to combine this reference with one or more other prior art references identified in Defendant's Invalidity Contentions Cover Pleading, particularly, § IV (B). Rather than repeat those disclosures here, they are incorporated by reference into this chart.
27. The system of claim 23, wherein the endpoint comprises a mobile device.	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim 5 which is incorporated by reference herein.
28. The system of claim 23, wherein the one or more software agents comprise at least one service provided by the operating system of the endpoint.	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim 6 which is incorporated by reference herein.
29. The system of claim 23, wherein the one or more	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation.

EXHIBIT E – CHENG

'038 Patent	Cheng
software agents comprise at least one application running on the endpoint.	For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim 7 which is incorporated by reference herein.
30. The system of claim 23, wherein the conditions comprise at least one hardware condition.	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim 8 which is incorporated by reference herein.
31. The system of claim 23, wherein the conditions comprise at least one software condition.	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim 9 which is incorporated by reference herein.
32. The system of claim 23, wherein the computing system comprises a plurality of servers.	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. For example, see the following passages and/or figures, as well as all related disclosures: <i>See above</i> re claim 10 which is incorporated by reference herein.
33. The system of claim 23, wherein the plurality of policies includes at least one policy that includes the at	Cheng discloses this claim limitation explicitly, inherently, or as a matter of common sense, or it would have been obvious to add missing aspects of the limitation. For example, see the following passages and/or figures, as well as all related disclosures:

EXHIBIT E – CHENG

'038 Patent	Cheng
least one rule that identifies the action.	<i>See above</i> re claim 11 which is incorporated by reference herein.