US007966650B2

(12) **United States Patent**
Manring et al.

(10) **Patent No.: US 7,966,650 B2**
(45) **Date of Patent: Jun. 21, 2011**

(54) **DYNAMIC INTERNET ADDRESS ASSIGNMENT BASED ON USER IDENTITY AND POLICY COMPLIANCE**

(75) Inventors: **Bradley A. C. Manring**, Dublin, OH (US); **Kenneth E. Mulh**, Upper Arlington, OH (US)

(73) Assignee: **Sophos PLC**, Abingdon (GB)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 790 days.

(21) Appl. No.: **12/035,638**

(22) Filed: **Feb. 22, 2008**

(65) **Prior Publication Data**

US 2009/0217350 A1 Aug. 27, 2009

(51) **Int. Cl.**

G06F 7/04	(2006.01)
G06F 15/16	(2006.01)
G06F 17/30	(2006.01)
H04L 29/06	(2006.01)

(52) **U.S. Cl.** **726/3**; 709/229

(58) **Field of Classification Search** 726/3; 709/229
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

7,249,187	B2	7/2007	Sobel	
7,586,912	B2 *	9/2009	Agarwal et al.	370/389
7,600,113	B2 *	10/2009	Kuehnel et al.	713/155
7,761,539	B2 *	7/2010	Izutani	709/222
7,844,718	B2 *	11/2010	Polcha et al.	709/229
2007/0011268	A1	1/2007	Banga et al.	
2007/0061458	A1	3/2007	Lum	
2009/0217346	A1 *	8/2009	Manring et al.	726/1
2009/0217350	A1 *	8/2009	Manning et al.	726/3

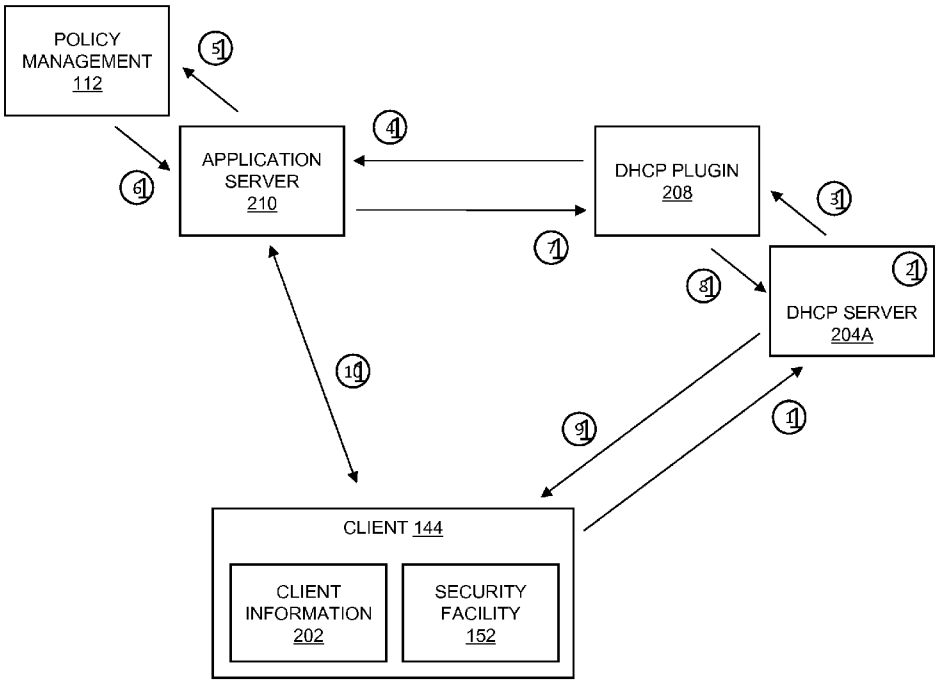
* cited by examiner

Primary Examiner — Farid Homayounmehr
(74) *Attorney, Agent, or Firm* — Strategic Patents, P.C.

(57) **ABSTRACT**

In embodiments of the present invention, improved capabilities are described for a method presenting a client, providing client information and requesting an IP address from a DHCP server, where the DHCP server may formulate a first IP assignment and a first multiple DHCP options. A policy management facility may be associated with the interception of the first IP assignment and the first multiple DHCP options, which may result in the first IP assignment and the first multiple DHCP options not being sent to the client. The method may send client information to the policy management facility. The policy management facility may formulate a second multiple DHCP options and may send it to the DHCP server. The DHCP server may change first IP assignment and first multiple DHCP option to a second IP assignment and the second multiple DHCP options. The second IP assignment and the second multiple DHCP options may then be forwarded to the client.

64 Claims, 5 Drawing Sheets



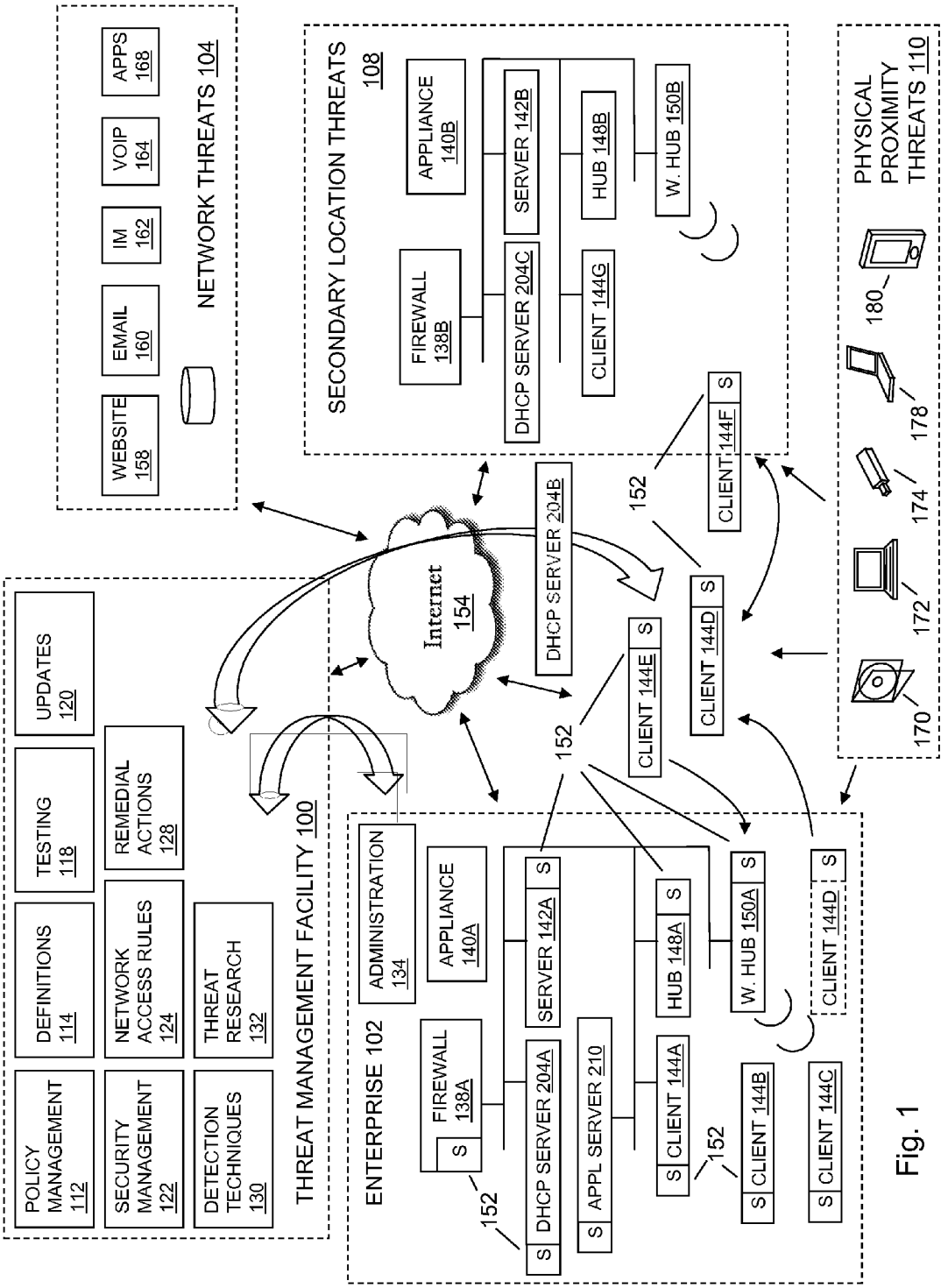

NETWORK THREATS 104
WEBSITE 158
EMAIL 160
IM 162
VOIP 164
APPS 168
SECONDARY LOCATION THREATS 108
FIREWALL 138B
APPLIANCE 140B
DHCP SERVER 204C
SERVER 142B
CLIENT 144G
HUB 148B
W. HUB 150B
CLIENT 144F
S
PHYSICAL PROXIMITY THREATS 110
170
172
174
178
180
Internet 154
DHCP SERVER 204B
152
CLIENT 144E
CLIENT 144D
THREAT MANAGEMENT FACILITY 100
POLICY MANAGEMENT 112
DEFINITIONS 114
TESTING 118
UPDATES 120
SECURITY MANAGEMENT 122
NETWORK ACCESS RULES 124
REMEDIAL ACTIONS 128
DETECTION TECHNIQUES 130
THREAT RESEARCH 132
ENTERPRISE 102
ADMINISTRATION 134
FIREWALL 138A
APPLIANCE 140A
DHCP SERVER 204A
SERVER 142A
APPL SERVER 210
HUB 148A
W. HUB 150A
CLIENT 144A
CLIENT 144B
CLIENT 144C
CLIENT 144D

Fig. 1

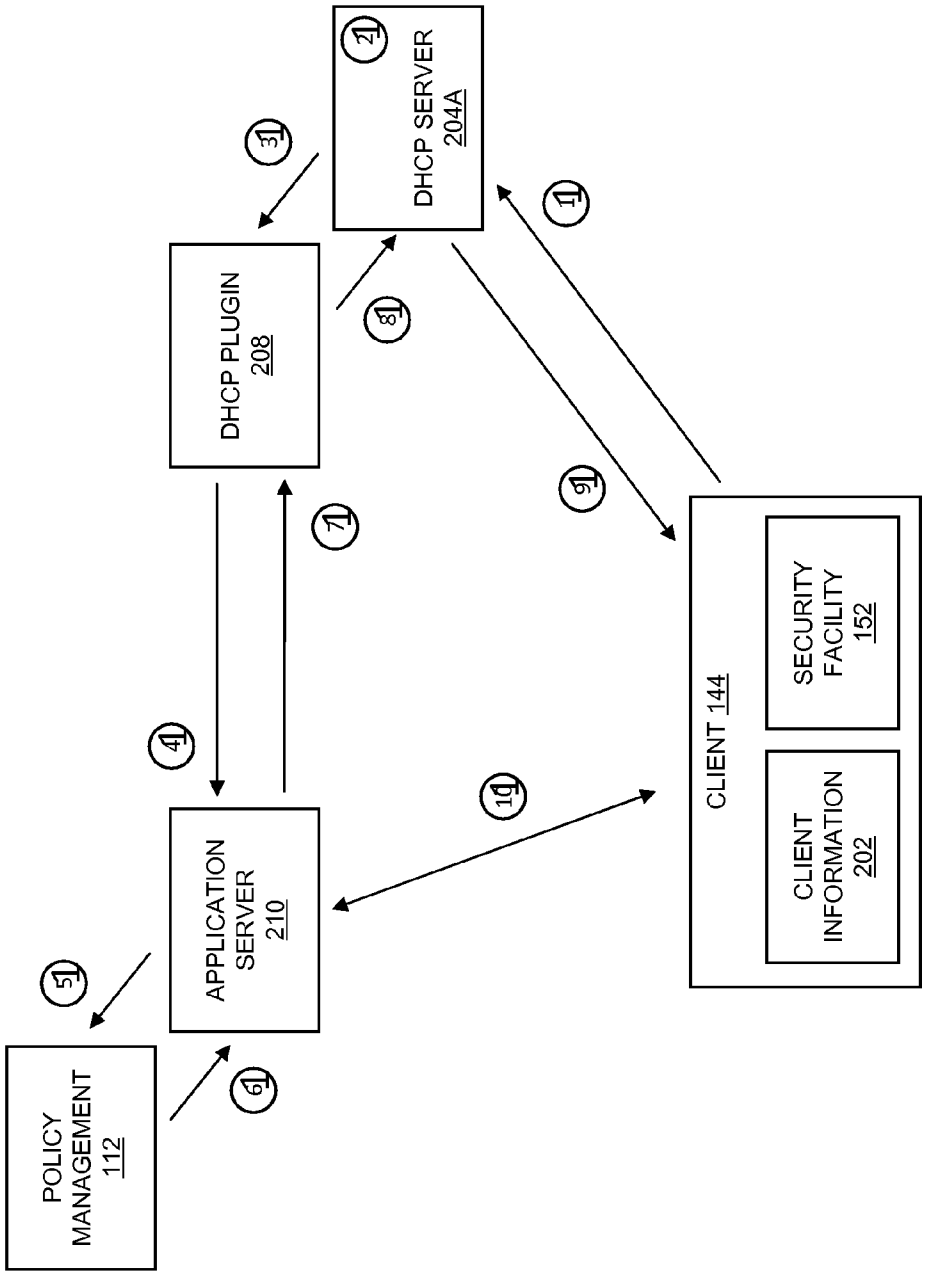

POLICY MANAGEMENT 112
APPLICATION SERVER 210
DHCP PLUGIN 208
DHCP SERVER 204A
CLIENT 144
SECURITY FACILITY 152
CLIENT INFORMATION 202
1
2
3
4
5
6
7
8
9
10
11

Fig. 2

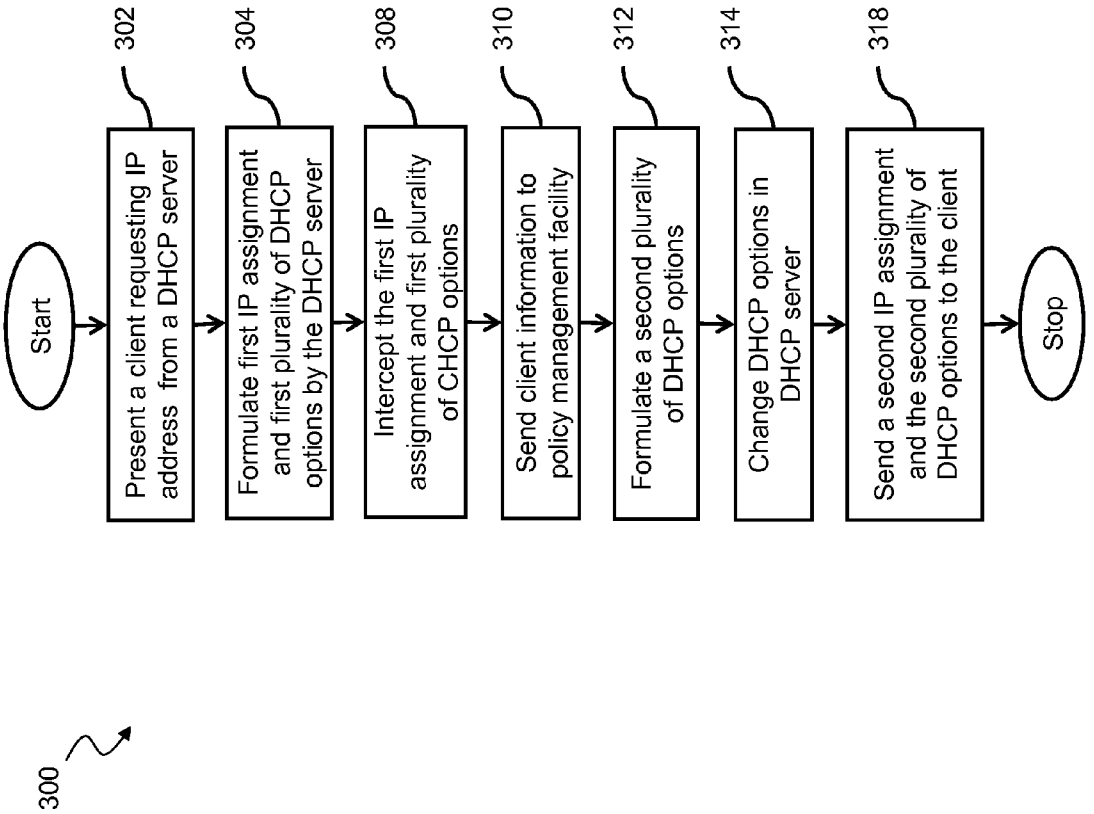

300
Start
302
Present a client requesting IP address from a DHCP server
304
Formulate first IP assignment and first plurality of DHCP options by the DHCP server
308
Intercept the first IP assignment and first plurality of CHCP options
310
Send client information to policy management facility
312
Formulate a second plurality of DHCP options
314
Change DHCP options in DHCP server
318
Send a second IP assignment and the second plurality of DHCP options to the client
Stop

Fig. 3

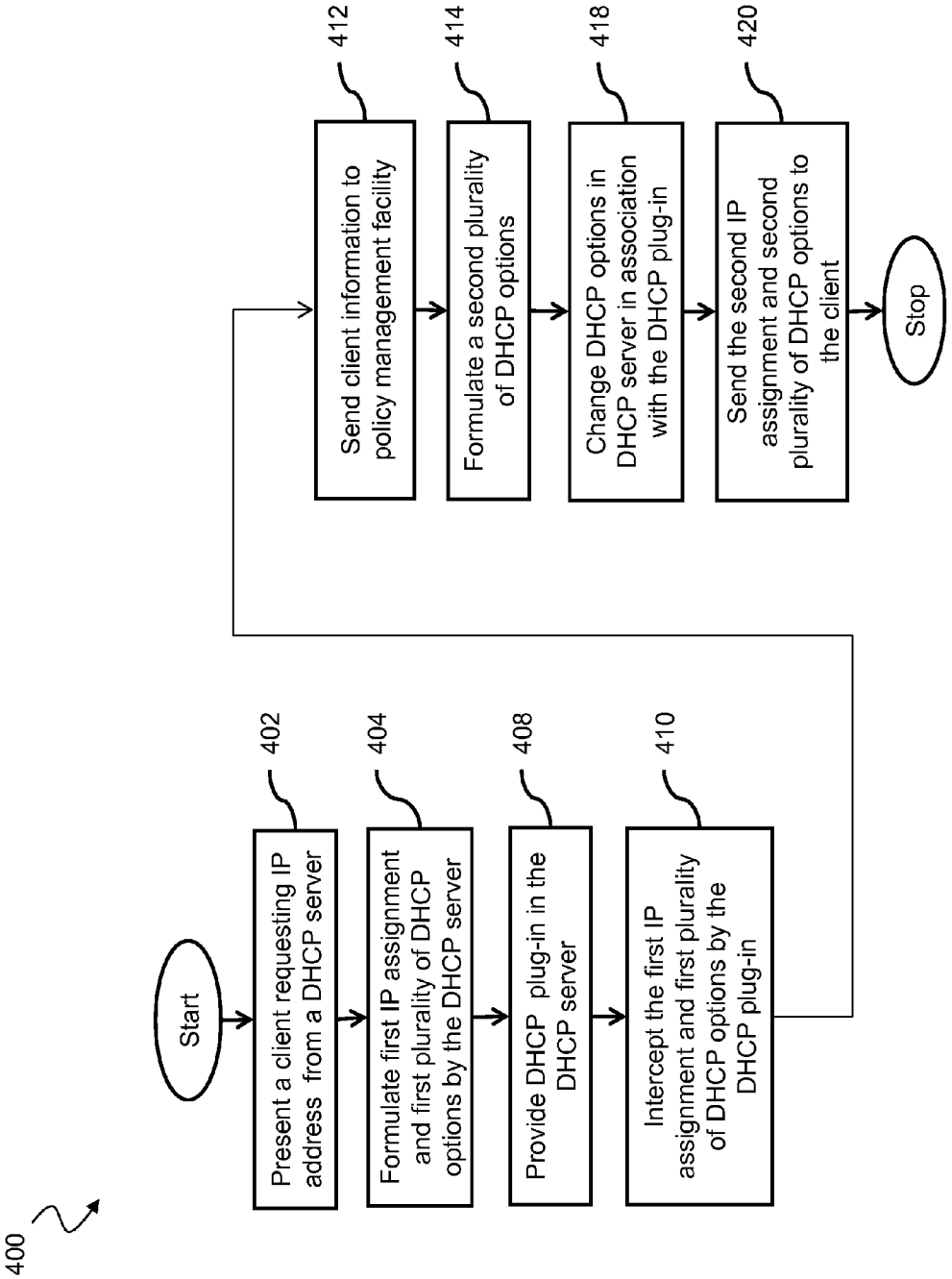

400
Start
402
Present a client requesting IP address from a DHCP server
404
Formulate first IP assignment and first plurality of DHCP options by the DHCP server
408
Provide DHCP plug-in in the DHCP server
410
Intercept the first IP assignment and first plurality of DHCP options by the DHCP plug-in
412
Send client information to policy management facility
414
Formulate a second plurality of DHCP options
418
Change DHCP options in DHCP server in association with the DHCP plug-in
420
Send the second IP assignment and second plurality of DHCP options to the client
Stop

Fig. 4

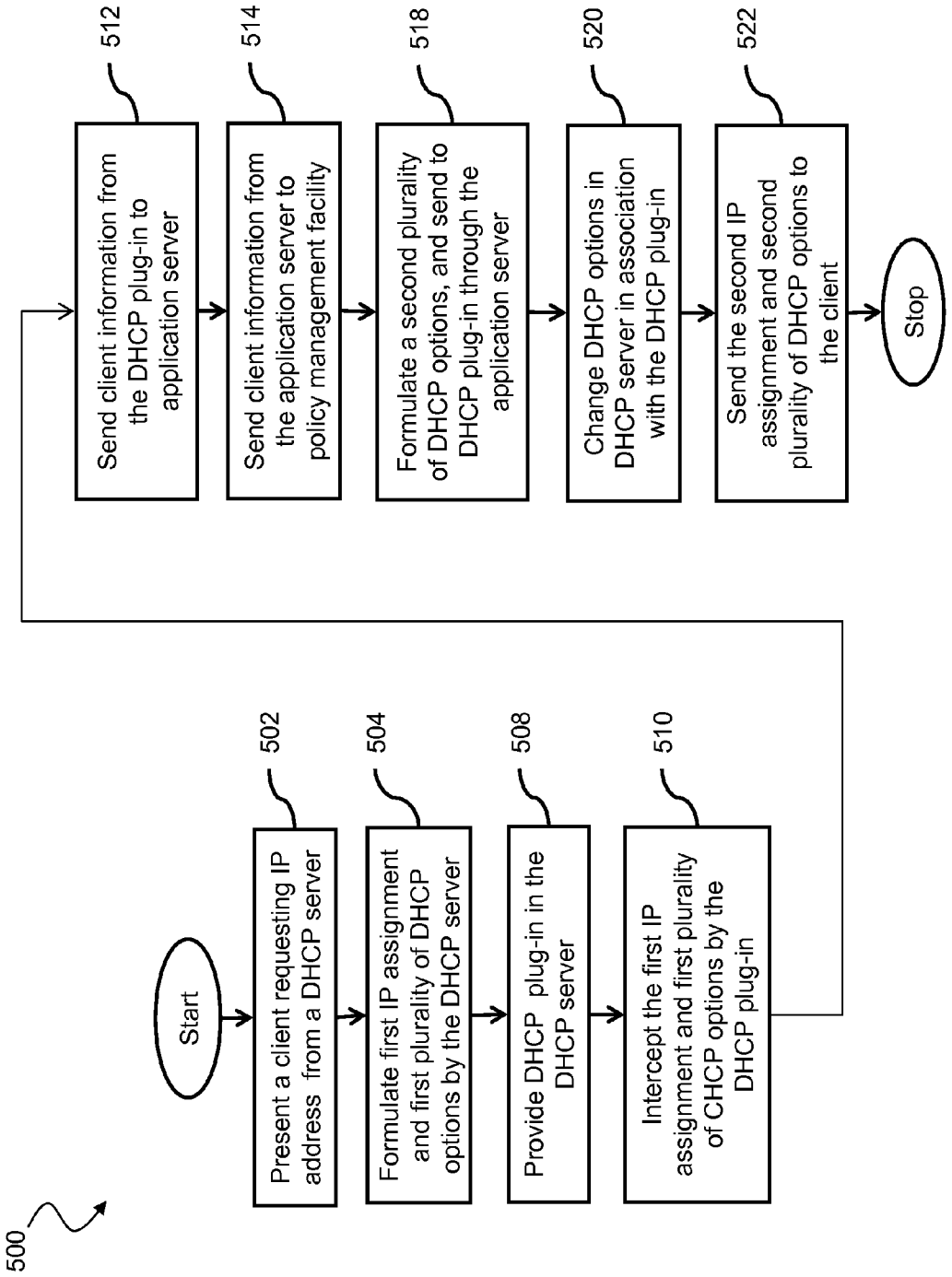

500
Start
502
Present a client requesting IP address from a DHCP server
504
Formulate first IP assignment and first plurality of DHCP options by the DHCP server
508
Provide DHCP plug-in in the DHCP server
510
Intercept the first IP assignment and first plurality of CHCP options by the DHCP plug-in
512
Send client information from the DHCP plug-in to application server
514
Send client information from the application server to policy management facility
518
Formulate a second plurality of DHCP options, and send to DHCP plug-in through the application server
520
Change DHCP options in DHCP server in association with the DHCP plug-in
522
Send the second IP assignment and second plurality of DHCP options to the client
Stop

Fig. 5

DYNAMIC INTERNET ADDRESS ASSIGNMENT BASED ON USER IDENTITY AND POLICY COMPLIANCE

BACKGROUND

1. Field

The present invention is related to secure computing, and more specifically to IP address assignment and DHCP options assignment to a client.

2. Description of the Related Art

A client, when connecting to an Internet Protocol (IP) network, requests an IP address from a Dynamic Host Configuration Protocol (DHCP) server. The responding DHCP server then assigns an IP address to the client. The DHCP server also assigns DHCP options to the client that are necessary for the client to operate on an IP network. Both the IP address and the DHCP options are then transmitted back to the client, which allows the client to operate on the IP network. Since the assignment is not tied to any policy rule associated with the client or to the user, the assignments are made automatically. This may be an issue if the client or the user poses a threat to network components or network accessible enterprise resources. There exists therefore a need for improved ways to assign IP addresses and DHCP options to a client.

SUMMARY

In embodiments of the present invention, improved capabilities are described for a dynamic internet address assignment based on user identity and policy compliance. The method includes presenting a client may request an IP address from a DHCP server, wherein the client may provide client information to the DHCP server; formulate a first IP assignment and a first multiple DHCP options by the DHCP server; intercept the first IP assignment and the first multiple DHCP options by a policy management facility, wherein intercepting may stop the sending of the first IP assignment and the first multiple DHCP options to the client; send client information to the policy management facility; formulate a second multiple DHCP options in association with the policy management facility, wherein the second multiple DHCP options may be sent from the policy management facility to the DHCP server; change the DHCP options in the DHCP server from the first IP assignment and first multiple DHCP options to a second IP assignment and the second multiple DHCP options; and send the second IP assignment and the second multiple DHCP options from the DHCP server to the client, wherein the client may apply the second IP assignment and the second multiple DHCP options in association with a client security facility.

In embodiments, the client request may be made when the client initializes the network, first connects to the network, boots up, or the like. In embodiments, the client request may be made in association with a lease, a security threat detected by the client end-point security facility, or the like. In embodiments, the client request for an IP address may be generated through a TCP/IP configured software resident on the client.

In embodiments, the DHCP server may implement a protocol used by the client to obtain parameters necessary for the client to operate on an internet protocol (IP) network. The parameter may be an IP address, a subnet mask, a default gateway, a lease, a TCP/IP configuration parameter, or some other type of parameter. Further, in embodiments, the lease may be associated with a length of time for which the IP address is allocated. Furthermore, the lease may be renewed.

In embodiments, the client may send a broadcast query to the network requesting the parameters from the DHCP server. Further, in embodiments, the broadcast query may be a discovery of the physical subnet to find available DHCP servers. In addition, the client may send the broadcast query when the client performs network initialization or when the client boots up.

In embodiments, the DHCP server may provide for a dynamic allocation of IP addresses. Further, the dynamic allocation may provide for a range of IP addresses. Furthermore, the range of IP address may be assigned by an administrator. In embodiments, the dynamic allocation may utilize the lease. Further, the lease may represent the time period for which the IP address may be valid.

In embodiments, the DHCP server may manage a number of IP addresses. Further, IP addresses may have been allocated. Furthermore, in embodiments, the allocation may be by an internet assigned numbers authority, a regional internet registry, an enterprise administrator or some other type of allocation. In embodiments, the IP address may be a unique address for network components of an IP network. Further, the IP address enables network components to communicate a unique address for the Internet, a unique address for a specific network, a unique address for an enterprise, a private IP address, or some other type of IP address.

In embodiments, multiple DHCP options are used to assign network configuration parameters. Further, the configuration may be automatic. In addition, the configuration may be for IP hosts. In embodiments, the network configuration parameter may be associated with a full network access, a normal network, a restricted access, or some other type of network configuration parameters. Furthermore, the restricted access may provide only external network access. In embodiments, the network configuration parameter may be associated with isolating the client. The isolated client may be associated with quarantine.

In embodiments, the network configuration parameter may be a subnet mask, a router, a time server, a name server, a domain server, a log server, a quotes server, a LPR server, an impress server, a RLP server, a hostname, a domain name, a static route, a vendor specific, an address request, an address time, a class ID, a client ID, a relay agent information, a classless static route, an IEE 802.1Q VLAN ID, or some other type of network configuration parameters.

In embodiments, the client information may be provided from the client to the DHCP server. Further, the client information may be provided by the client as a part of the client request for an IP address, In addition, the client information may be provided automatically as a part of the client request for the IP address or when the DHCP server may request the client information. Furthermore, the DHCP server request may be made each time a client requests an IP address, in association with a DHCP plug-in, may be initiated by the DHCP plug-in, and the like.

In embodiments, the client information may be a MAC address, a time of day, a current location of the client, a user ID, a user name, an IP address requested by the client, a DHCP option requested by the client, a client capability, or some other type of client information. Further, the client capability may be the presence of a software application, a network access control capability, or some other type of client capability.

In embodiments, the client information may be security vulnerability. Further, the security vulnerability may be associated with malware security vulnerability. In embodiments, the malware security vulnerability may be from the client having no end-point security facility or out of date end-point

security facility. Furthermore, the end-point security facility may be malware security software.

In embodiments the malware security vulnerability may be from the client end-point security facility detecting a malware threat, a suspicious behavior, associated with a client end-point firewall, and the like. Further, there may be no client end-point firewall or the client end-point firewall may be improperly configured.

In embodiments, the client information may be software vulnerability. Further, the software vulnerability may be associated with a license, a registration, an unauthorized software application, or some other type of software vulnerability. Furthermore, the license may be out of date or there may be no valid license agreement. In embodiments, the registration may be out of date or there may be no valid registration.

In embodiments, the client information may be a client configuration status. Further, the client configuration status may be associated with the policy management facility, the client operating system, the client end-point security facility, or some other type of client configuration status. Furthermore, in embodiments, the policy management facility may read the configuration status as an indication of policy compliance.

In embodiments, interception may be provided by the DHCP plug-in, the application server, the policy management facility, or some other type of mechanism.

In embodiments, formulating the second multiple DHCP options in association with the policy management facility may be in association with a policy. Further, the policy may be associated with user identification, a client configuration, an end-point security status, a location, a time or some other type of policy, and the like.

In embodiments, the user identification may be associated with an enterprise organizational set of policies, employment status, personal policy profile, or some other type of user identification. Further, the enterprise organizational set of policies may be associated with a department, a management position within the enterprise, a personnel position within the enterprise, an outside contractor, a visitor to the enterprise, or some other type of parameter.

In embodiments, the policy may be associated with the client configuration. The client configuration may be associated with compliance, a client capability, and the like. Further, the compliance may be end-point security compliance. Furthermore, the end-point security compliance may be associated with the client having updated end-point security software. In embodiments, the compliance may be a software application compliance, a hardware compliance, a registration compliance, a license compliance, or some other type of compliance. In embodiment, the client configuration may be associated with the client capability. Further, the client capability may be a software capability, a hardware capability, a network access capability, an interface capability, or some other type of client capability.

In embodiments, the policy may be associated with an end-point security status. Further, the end-point security status may indicate detection of malware or of suspicious behavior. The suspicious behavior may be associated with a software file or a user action.

In embodiments, the policy may be associated with a location. The location may be a current location, the home location, the previous location, a geographic location, an enterprise location, a personal location, a mobile location, or some other type of location.

In embodiments, the policy may be associated with a time. The time may be associated with work hours. In addition, the time may be during normal work hours, after work hours, late night, or some other time.

In embodiments of the present invention, improved capabilities are described for dynamic internet address assignment and policy compliance. The method may present the client requesting an IP address from a DHCP server, wherein the client may provide client information to the DHCP server; formulate the first IP assignment and a first multiple DHCP options by the DHCP server; provide a DHCP plug-in in the DHCP server; intercept the first IP assignment and the first multiple DHCP options by the DHCP plug-in, wherein intercepting may stop the sending of the first IP assignment and the first multiple DHCP options to the client; send client information to a policy management facility through the DHCP plug-in; formulate the second multiple DHCP options in association with the policy management facility, wherein the second multiple DHCP options may be sent from the policy management facility to the DHCP plug-in; change the DHCP options in the DHCP server from the first IP assignment and first multiple DHCP options to a second IP assignment and the second multiple DHCP options in association with the DHCP plug-in and sends the second IP assignment and the second multiple DHCP options from the DHCP server to the client, wherein the client applies the second IP assignment and the second multiple DHCP options in association with a client security facility.

In embodiments of the present invention, improved capabilities are described for dynamic internet address assignment and policy compliance. The method may presents the client requesting an IP address from the DHCP server, wherein the client may provide client information to the DHCP server; formulate the first IP assignment and the first multiple DHCP options by the DHCP server; provide the DHCP plug-in in the DHCP server, wherein the DHCP plug-in acts as an application server client to an application server; intercept the first IP assignment and the first multiple DHCP options by the DHCP plug-in, wherein intercepting stops the sending of the first IP assignment and the first multiple DHCP options to the client; send client information from the DHCP plug-in to the application server; send client information from the application server to a policy management facility; formulate a second multiple DHCP options in association with the policy management facility, wherein the second multiple DHCP options is sent from the policy management facility to the DHCP plug-in through the application server; change the DHCP options in the DHCP server from the first IP assignment and first multiple DHCP options to a second IP assignment and the second multiple DHCP options in association with the DHCP plug-in; and send the second IP assignment and the second multiple DHCP options from the DHCP server to the client, wherein the client applies the second IP assignment and the second multiple DHCP options in association with a client security facility.

BRIEF DESCRIPTION OF THE FIGURES

The invention and the following detailed description of certain embodiments thereof may be understood by reference to the following figures:

FIG. **1** depicts a block diagram of the threat management facility providing protection to an enterprise against a plurality of threats.

FIG. **2** shows a process flow embodiment for dynamic internet address assignment based on user identity and policy compliance.

FIG. **3** shows a process flow embodiment for dynamic internet address assignment based on user identity and policy compliance without a DHCP plug-in.

FIG. **4** shows a process flow embodiment for dynamic internet address assignment based on user identity and policy compliance by adding a DHCP plug-in.

FIG. **5** shows a process flow embodiment for dynamic internet address assignment based on user identity and policy compliance by adding a DHCP plug-in and application server.

While the invention has been described in connection with certain preferred embodiments, other embodiments would be understood by one of ordinary skill in the art and are encompassed herein.

All documents referenced herein are hereby incorporated by reference.

DETAILED DESCRIPTION

An aspect of the present invention relates to corporate policy management and their implementation through a threat management facility **100**. As will be explained in more detail below, a threat management facility **100** is used to protect computer assets from many threats, both computer generated threats and user generated threats. The threat management facility **100** is multi-dimensional in that it is designed to protect corporate assets from a variety of threats and it is adapted to learn about threats in one dimension (e.g. worm detection) and apply the knowledge in another dimension (e.g. spam detection). Corporate policy management is one of the dimensions for which the threat management facility can control. The corporation may institute a policy that prevents certain people (e.g. employees, groups of employees, types of employees, guest of the corporation, etc.) from accessing certain types of computer programs. For example, the corporation may elect to prevent its accounting department from using a particular version of an instant messaging service or all such services. In this example, the policy management facility **112** may be used to update the policies of all corporate computing assets with a proper policy control facility or it may update a select few. By using the threat management facility **100** to facilitate the setting, updating and control of such policies the corporation only needs to be concerned with keeping the threat management facility **100** up to date on such policies. The threat management facility **100** can take care of updating all of the other corporate computing assets.

It should be understood that the threat management facility **100** may provide multiple services and policy management may be offered as one of the services. We will now turn to a description of the threat management system **100**.

Over recent years, malware has become a major problem across the internet **154**. From both technical and user perspectives the categorization of a specific threat type, such as whether it is a virus, worm, spam, phishing exploration, spyware, adware, or the like, is becoming reduced in significance. The threat, no matter how it's categorized, may need to be stopped at all points of the enterprise facility **102**, including laptop, desktop, server facility **142**, gateway, and the like. Similarly, there may be less and less benefit to the user in having different solutions for known and unknown threats. As such, a consolidated threat management facility **100** may need to be applied to the same set of technologies and capabilities for all threats. The threat management facility **100** may provide a single agent on the desktop, and a single scan of any suspect file. This approach may eliminate the inevitable overlaps and gaps in protection caused by treating viruses and spyware as separate problems, while simultaneously simplifying administration and minimizing desktop load. As the number and range of types of threats has increased, so may have the level of connectivity available to all IT users. This may have lead to a rapid increase in the speed at which threats may move. Today, an unprotected PC connected to the internet **154** may be infected quickly, say within 10 minutes, which may require acceleration for the delivery of threat protection. Where once, monthly updates may have been sufficient, the threat management facility **100** may automatically and seamlessly update its product set against spam and virus threats quickly, for instance, every five minutes, every minute, continuously, or the like. Analysis and testing may be increasingly automated, and also may be performed more frequently; for instance, it may be completed in 15 minutes, and may do so without compromising quality. The threat management facility **100** may also extend techniques that may have been developed for virus and malware protection, and provide them to enterprise facility **102** network administrators to better control their environments. In addition to stopping malicious code, the threat management facility **100** may provide policy management that may be able to control legitimate applications, such as VoIP, instant messaging, peer-to-peer file-sharing, and the like, that may undermine productivity and network performance within the enterprise facility **102**.

The threat management facility **100** may provide an enterprise facility **102** protection from computer-based malware, including viruses, spyware, adware, Trojans, intrusion, spam, policy abuse, uncontrolled access, and the like, where the enterprise facility **102** may be any entity with a networked computer-based infrastructure. In an embodiment, FIG. **1** may depict a block diagram of the threat management facility providing protection to an enterprise against a plurality of threats. The enterprise facility **102** may be corporate, commercial, educational, governmental, or the like, and the enterprise facility's **102** computer network may be distributed amongst a plurality of facilities, and in a plurality of geographical locations. The threat management facility **100** may include a plurality of functions, such as security management facility **122**, policy management facility **112**, update facility **120**, definitions facility **114**, network access rules facility **124**, remedial action facility **128**, detection techniques facility **130**, testing facility **118**, threat research facility **132**, and the like. In embodiments, the threat protection provided by the threat management facility **100** may extend beyond the network boundaries of the enterprise facility **102** to include enterprise facility **102** client facility's **144** that have moved into network connectivity not directly associated or controlled by the enterprise facility **102**. Threats to enterprise facility **102** client facilities **144** may come from a plurality of sources, such as from network threats **104**, physical proximity threats **110**, secondary location threats **108**, and the like. In embodiments, the threat management facility **100** may provide an enterprise facility **102** protection from a plurality of threats to multiplatform computer resources in a plurality of locations and network configurations, with an integrated system approach.

In embodiments, the threat management facility **100** may be provided as a stand-alone solution. In other embodiments, the threat management facility **100** may be integrated into a third-party product. An application programming interface (e.g. a source code interface) may be provided such that the threat management facility **100** may be integrated. For instance, the threat management facility **100** may be stand-alone in that it provides direct threat protection to an enterprise or computer resource, where protection is subscribed to directly with the threat management facility **100**. Alterna-

tively, the threat management facility may offer protection indirectly, through a third-party product, where an enterprise may subscribe to services through the third-party product, and threat protection to the enterprise may be provided by the threat management facility **100** through the third-party product.

The security management facility **122** may include a plurality of elements that provide protection from malware to enterprise facility **102** computer resources, including end-point security and control, email security and control, web security and control, control of unauthorized users, control of guest and non-compliant computers, and the like. The security management facility **122** may be a software application that may provide malicious code and malicious application protection to a client facility **144** computing resource. The security management facility **122** may have the ability to scan the client facility **144** files for malicious code, remove or quarantine certain applications and files, prevent certain actions, perform remedial actions and perform other security measures. In embodiments, scanning the client facility **144** may include scanning some or all of the files stored to the client facility **144** on a periodic basis, may scan applications once the application has been requested to execute, may scan files as the files are transmitted to or from the client facility **144**, or the like. The scanning of the applications and files may be to detect known malicious code or known unwanted applications. In an embodiment, new malicious code and unwanted applications may be continually developed and distributed, and updates to the known code database may be provided on a periodic basis, on a demand basis, on an alert basis, or the like.

In an embodiment, the security management facility **122** may provide for email security and control, where security management may help to eliminate spam, viruses, spyware and phishing, control of email content, and the like. The security management facilities **122** email security and control may protect against inbound and outbound threats, protect email infrastructure, prevent data leakage, provide spam filtering, and the like. In an embodiment, security management facility **122** may provide for web security and control, where security management may help to detect or block viruses, spyware, malware, unwanted applications, help control web browsing, and the like, which may provide comprehensive web access control enabling safe, productive web browsing. Web security and control may provide internet use policies, reporting on suspect devices, security and content filtering, active monitoring of network traffic, URL filtering, and the like. In an embodiment, the security management facility **122** may provide for network access control, which may provide control over network connections. Network control may stop unauthorized, guest, or non-compliant systems from accessing networks, and may control network traffic that may not be bypassed from the client level. In addition, network access control may control access to virtual private networks (VPN), where VPNs may be a communications network tunneled through another network, establishing a logical connection acting as a virtual network. In embodiments, a VPN may be treated in the same manner as a physical network.

In an embodiment, the security management facility **122** may provide for host intrusion prevention through behavioral based protection, which may guard against unknown threats by analyzing behavior before software code executes. Behavioral based protection may monitor code when it runs and intervene if the code is deemed to be suspicious or malicious. Advantages of behavioral based protection over runtime protection may include code being prevented from running, whereas runtime protection may only interrupt code that has already partly executed; behavioral protection may identify malicious code at the gateway or on the file servers and deletes it before reaching end-point computers; and the like.

In an embodiment, the security management facility **122** may provide for reputation filtering, which may target or identify sources of known malware. For instance, reputation filtering may include lists of URLs of known sources of malware or known suspicious IP addresses, or domains, say for spam, that when detected may invoke an action by the threat management facility **100**, such as dropping them immediately. By dropping the source before any interaction can initiate, potential threat sources may be thwarted before any exchange of data can be made.

In embodiments, information may be sent from the enterprise back to a third party, a vendor, or the like, which may lead to improved performance of the threat management facility **100**. For example, the types, times, and number of virus interactions that a client experiences may provide useful information for the preventions of future virus threats. This type of feedback may be useful for any aspect of threat detection. Feedback of information may also be associated with behaviors of individuals within the enterprise, such as being associated with most common violations of policy, network access, unauthorized application loading, unauthorized external device use, and the like. In embodiments, this type of information feedback may enable the evaluation or profiling of client actions that are violations of policy that may provide a predictive model for the improvement of enterprise policies.

In an embodiment, the security management facility **122** may provide for the overall security of the enterprise facility **102** network or set of enterprise facility **102** networks, may provide updates of malicious code information to the enterprise facility **102** network, and associated client facilities **144**. The updates may be a planned update, an update in reaction to a threat notice, an update in reaction to a request for an update, an update based on a search of known malicious code information, or the like. The administration facility **134** may provide control over the security management facility **122** when updates are performed. The updates may be automatically transmitted without an administration facility's **134** direct control, manually transmitted by the administration facility **134**, or the like. The security management facility **122** may include the management of receiving malicious code descriptions from a provider, distribution of malicious code descriptions to enterprise facility **102** networks, distribution of malicious code descriptions to client facilities **144**, or the like. In an embodiment, the management of malicious code information may be provided to the enterprise facility's **102** network, where the enterprise facility's **102** network may provide the malicious code information through the enterprise facility's **102** network distribution system.

The threat management facility **100** may provide policy management facility **112** that may be able to block non-malicious applications, such as VoIP **164**, instant messaging **162**, peer-to-peer file-sharing, and the like, that may undermine productivity and network performance within the enterprise facility **102**. The policy management facility **112** may be a set of rules or policies that may indicate enterprise facility **102** access permissions for the client facility **144**, such as access permissions associated with the network, applications, external computer devices, and the like. The policy management facility **112** may include a database, a text file, a combination of databases and text files, or the like. In an embodiment, a policy database may be a block list, a black list, an allowed list, a white list, or the like that may provide a list of enterprise facility **102** external network locations/applications that may or may not be accessed by the client facility

144. The policy management facility 112 may include rules that may be interpreted with respect to an enterprise facility 102 network access request to determine if the request should be allowed. The rules may provide a generic rule for the type of access that may be granted; the rules may be related to the policies of an enterprise facility 102 for access rights for the enterprise facility's 102 client facility 144. For example, there may be a rule that does not permit access to sporting websites. When a website is requested by the client facility 144, a security facility may access the rules within a policy facility to determine if the requested access is related to a sporting website. In an embodiment, the security facility may analyze the requested website to determine if the website matches with any of the policy facility rules.

The policy management facility 112 may be similar to the security management facility 122 but with the distribution of enterprise facility 102 wide access rules and policies that may maintain control of the access of client facility 144 to enterprise facility 102 network resources. The policies may be defined for application type, subset of application capabilities, organization hierarchy, computer facility type, user type, network location, time of day, connection type, or the like. Policies may be maintained by the administration facility 134, through the threat management facility 100, in association with a third party, or the like. For example, a policy may restrict IM 162 activity to only support personnel for communicating with customers. This may allow communication for departments requiring access, but may maintain the network bandwidth for other activities by restricting the use of IM 162 to only the personnel that need access to IM 162 in support of the enterprise facility 102. In an embodiment, the policy management facility 112 may be a standalone application, may be part of the policy management facility 112 network server facility 142, may be part of the enterprise facility 102 network, may be part of the client facility 144, or the like.

In embodiments, the threat management facility 100 may provide configuration management, which may be similar to policy management, but may specifically examine the configuration set of applications, operating systems, hardware, and the like, and managing changes to their configurations. Assessment of a configuration may be made against a standard configuration policy, detection of configuration changes, remediation of improper configuration, application of new configurations, and the like. An enterprise may keep a set of standard configuration rules and policies which may represent the desired state of the device. For example, a client firewall may be running and installed, but in the disabled state, where remediation may be to enable the firewall. In another example, the enterprise may set a rule that disallows the use of USB disks, and sends a configuration change to all clients, which turns off USB drive access via a registry.

In embodiments, the threat management facility 100 may also provide for the removal of applications that may interfere with the operation of the threat management facility 100, such as competitor products that may also be attempting similar threat management functions. The removal of such products may be initiated automatically whenever such products are detected. In the case where such applications are services are provided indirectly through a third-party product, the application may be suspended until action is taken to remove or disable the third-party product's protection facility.

Threat management against a sometimes quickly evolving malware environment may require timely updates, and the update management facility 120 may be provided by the threat management facility 100.enterprise facility 102. In addition, a policy management facility 112 may also require update management (e.g. as provided by the update facility 120 herein described), as the enterprise facility 102 requirements for policies change enterprise facility 102 server facility 142 enterprise facility 102 client facility 144 server facility 142 enterprise facility 102. The update management for the security facility 122 and policy management facility 112 may be provided directly by the threat management facility 100, such as by a hosted system or in conjunction with the administration facility 134. In embodiments, the threat management facility 100 may provide for patch management, where a patch may be an update to an operating system, an application, a system tool, or the like, where one of the reasons for the patch is to reduce vulnerability to threats.

In embodiments, the security facility 122 and policy management facility 112 may push information to the enterprise facility 102 network and/or client facility 144, the enterprise facility 102 network and/or client facility 144 may pull information from the security facility 122 and policy management facility 112 network server facilities 142, there may be a combination of pushing and pulling of information between the security facility 122 and the policy management facility 112 network servers 142, enterprise facility 102 network, and client facilities 144, or the like. For example, the enterprise facility 102 network and/or client facility 144 may pull information from the security facility 122 and policy management facility 112 network server facility 142 may request the information using the security facility 122 and policy management facility 112 update module; the request may be based on a certain time period, by a certain time, by a date, on demand, or the like. In another example, the security facility 122 and policy management facility 112 network servers 142 may push the information to the enterprise facility's 102 network and/or client facility 144 by providing notification that there are updates available for download and then transmitting the information. The combination of the security management 122 network server facility 142 and security update module may function substantially the same as the policy management facility 112 network server and policy update module by providing information to the enterprise facility 102 network and the client facility 144 in a push or pull method. In an embodiment, the policy management facility 112 and the security facility 122 management update modules may work in concert to provide all the needed information to the enterprise facility's 102 network and/or client facility 144 for control of application execution. In an embodiment, the policy update module and security update module may be combined into a single update module.

As threats are identified and characterized, the threat management facility 100 may create definition updates that may be used to allow the threat management facility 100 to detect and remediate the latest malicious software, unwanted applications, configuration and policy changes, and the like. The threat definition facility 114 may contain threat identification updates, also referred to as definition files. A definition file may be a virus identity file that may include definitions of known or potential malicious code. The IDE definition files may provide information that may identify malicious code within files, applications, or the like. The definition files may be accessed by security management facility 122 when scanning files or applications within the client facility 144 for the determination of malicious code that may be within the file or application. The definition files may contain a number of commands, definitions, or instructions, to be parsed and acted upon, or the like. In embodiments, the client facility 144 may be updated with new definition files periodically to provide the client facility 144 with the most recent malicious code definitions; the updating may be performed on a set time

period, may be updated on demand from the client facility **144**, may be updated on demand from the network, may be updated on a received malicious code alert, or the like. In an embodiment, the client facility **144** may request an update to the definition files from an update facility **120** within the network, may request updated definition files from a computing facility external to the network, updated definition files may be provided to the client facility **114** from within the network, definition files may be provided to the client facility **144** from an external computing facility from an external network, or the like.

In an embodiment, a definition management facility **114** may provide for the timely updates of definition files information to the network, client facilities **144**, and the like. New and altered malicious code and malicious applications may be continually created and distributed to networks worldwide. The definition files that maintain the definitions of the malicious code and malicious application information for the protection of the networks and client facilities **144** may need continual updating to provide continual defense of the network and client facility **144** from the malicious code and malicious applications. The definition files management may provide for automatic and manual methods of updating the definition files. In embodiments, the network may receive definition files and distribute the definition files to the network client facilities **144**, the client facilities **144** may receive the definition files directly, or the network and client facilities **144** may both receive the definition files, or the like. In an embodiment, the definition files may be updated on a fixed periodic basis, on demand by the network and/or the client facility **144**, as a result of an alert of a new malicious code or malicious application, or the like. In an embodiment, the definition files may be released as a supplemental file to an existing definition files to provide for rapid updating of the definition files.

In a similar manner, the security management facility **122** may be used to scan an outgoing file and verify that the outgoing file is permitted to be transmitted per the enterprise facility **102** rules and policies. By checking outgoing files, the security management facility **122** may be able discover malicious code infected files that were not detected as incoming files as a result of the client facility **144** having been updated with either new definition files or policy management facility **112** information. The definition files may discover the malicious code infected file by having received updates of developing malicious code from the administration facility **134**, updates from a definition files provider, or the like. The policy management facility **112** may discover the malicious code infected file by having received new updates from the administration facility **134**, from a rules provider, or the like.

The threat management facility **100** may provide for a way to control access to the enterprise facility **102** networks. For instance, the enterprise facility **102** may want to restrict access to certain applications, networks, files, printers, servers, databases, or the like. In addition, the enterprise facility **102** may want to restrict user access under certain conditions, such as the user's location, usage history, need to know, job position, connection type, time of day, method of authentication, client-system configuration, or the like. Network access rules may be developed by the enterprise facility **102**, or pre-packaged by a supplier, and managed by the threat management facility **100** in conjunction with the administration facility **134**. Network access rules and control may be responsible for determining if a client facility **144** application should be granted access to a requested network location. The network location may be on the same network as the facility or may be on another network. In an embodiment, the network access control may verify access rights for client facilities **144** from within the network or may verify access rights of computer facilities from external networks. When network access for a client facility **144** is denied, the network access control may send an information file to the client facility **144**, the information file may contain data or commands that may provide instructions for the remedial action facility **128**. The information sent by the network access facility **124** control may be a data file. The data file may contain a number of commands, definitions, instructions, or commands to be parsed and acted upon through the remedial action facility **128**, or the like. The information sent by the network access facility **124** control may be a command or command file that the remedial action facility **128** may access and take action upon.

In an embodiment, the network access rules **124** may provide an information store to be accessed by the network access control. The network access rules facility **124** may include databases such as a block list, a black list, an allowed list, a white list, an unacceptable network site database, an acceptable network site database, a network site reputation database, or the like of network access locations that may or may not be accessed by the client facility **144**. Additionally, the network access rules facility **124** may incorporate rule evaluation; the rule evaluation may parse network access requests and apply the parsed information to network access rules. The network access rule facility **124** may have a generic set of rules that may be in support of an enterprise facility's **102** network access policies, such as denying access to certain types of websites **158**, controlling instant messenger **162** accesses, or the like. Rule evaluation may include regular expression rule evaluation, or other rule evaluation method for interpreting the network access request and comparing the interpretation to the established rules for network access. In an embodiment, the network access rules facility **124** may receive a rules evaluation request from the network access control and may return the rules evaluation to the network access control.

Similar to the threat definitions facility **114**, the network access rule facility **124** may provide updated rules and policies to the network access rules facility **124**. The network access rules facility **124** may be maintained by the network administration facility **134** using the network access rules facility **124** management. In an embodiment, the network administration facility **134** may be able to maintain a set of access rules manually by adding rules, changing rules, deleting rules, or the like. Additionally, the administration facility **134** may be able to retrieve predefined rule sets from a provider that may provide a set of rules to be applied to an entire enterprise facility **102**. The network administration facility **134** may be able to modify the predefined rules as needed for a particular enterprise facility **102** using the network access rules facility **124** management.

When a threat or policy violation is detected by the threat management facility **100**, the threat management facility **100** may provide for a remedial action facility **128**. Remedial action may take a plurality of forms, such as terminating or modifying an ongoing process or interaction, sending a warning to a client or administration facility **134** of an ongoing process or interaction, executing a program or application to remediate against a threat or violation, record interactions for subsequent evaluation, or the like. Remedial action may be associated with an application that responds to information that a client facility **144** network access request has been denied. In an embodiment, when the data file is received, remedial action may parse the data file, interpret the various aspects of the data file, and act on the parsed data file infor-

mation to determine actions to be taken on an application requesting access to a denied network location. In an embodiment, when the data file is received, remedial action may access the threat definitions to parse the data file and determine an action to be taken on an application requesting access to a denied network location. In an embodiment, the information received from the facility may be a command or a command file. The remedial action facility may carry out any commands that are received or parsed from a data file from the facility without performing any interpretation of the commands. In an embodiment, the remedial action facility may interact with the received information and may perform various actions on a client requesting access to a denied network location. The action may be one or more of continuing to block all requests to a denied network location, a malicious code scan on the application, a malicious code scan on the client facility **144**, quarantine of the application, terminating the application, isolation of the application, isolation of the client facility **144** to a location within the network that restricts network access, blocking a network access port from a client facility **144**, reporting the application to a administration facility **134**, or the like.

Remedial action may be provided as a result of a detection of a threat or violation. The detection techniques facility **130** may include monitoring the enterprise facility **102** network or end-point devices, such as by monitoring streaming data through the gateway, across the network, through routers and hubs, and the like. The detection techniques facility **130** may include monitoring activity and stored files on computing facilities, such as on server facilities **142**, desktop computers, laptop computers, other mobile computing devices, and the like. Detection techniques, such as scanning a computer's stored files, may provide the capability of checking files for stored threats, either in the active or passive state. Detection techniques, such as streaming file management, may provide the capability of checking files received at the network, gateway facility, client facility **144**, and the like. This may provide the capability of not allowing a streaming file or portions of the streaming file containing malicious code from entering the client facility **144**, gateway facility, or network. In an embodiment, the streaming file may be broken into blocks of information, and a plurality of virus identities may be used to check each of the blocks of information for malicious code. In an embodiment, any blocks that are not determined to be clear of malicious code may not be delivered to the client facility **144**, gateway facility, or network.

Verifying that the threat management facility **100** is detecting threats and violations to established policy, may require the ability to test the system, either at the system level or for a particular computing component. The testing facility **118** may allow the administration facility **134** to coordinate the testing of the security configurations of client facility **144** computing facilities on a network. The administration facility **134** may be able to send test files to a set of client facility **144** computing facilities to test the ability of the client facility **144** to determine acceptability of the test file. After the test file has been transmitted, a recording facility may record the actions taken by the client facility **144** in reaction to the test file. The recording facility may aggregate the testing information from the client facility **144** and report the testing information to the administration facility **134**. The administration facility **134** may be able to determine the level of preparedness of the client facility **144** computing facilities by the reported information. Remedial action may be taken for any of the client facility **144** computing facilities as determined by the administration facility **134**; remedial action may be taken by the administration facility **134** or by the user of the client facility **144**.

The threat research facility **132** may provide a continuously ongoing effort to maintain the threat protection capabilities of the threat management facility **100** in light of continuous generation of new or evolved forms of malware. Threat research may include researchers and analysts working on known and emerging malware, such as viruses, rootkits a spyware, as well as other computer threats such as phishing, spam, scams, and the like. In embodiments, through threat research, the threat management facility **100** may be able to provide swift, global responses to the latest threats.

The threat management facility **100** may provide threat protection to the enterprise facility **102**, where the enterprise facility **102** may include a plurality of networked components, such as client facility **144**, server facility **142**, a dynamic host configuration protocol (DHCP) server **204**, an applications server **210**, administration facility **134**, firewall **138**, gateway, hubs **148**, routers, threat management appliance **140**, desktop users, mobile users, and the like. In embodiments, it may be the end-point computer security facility **152**, located on a computer's desktop, which may provide threat protection to a user, and associated enterprise facility **102**. The end-point computer security facility **152** may be an application loaded onto the computer platform or computer support component, where the application may accommodate the plurality of computer platforms and/or functional requirements of the component. For instance, a client facility **144** computer may be one of a plurality of computer platforms, such as Windows, Macintosh, Linux, and the like, where the end-point computer security facility **152** may be adapted to the specific platform, while maintaining a uniform product and product services across platforms. Additionally, components may have different functions to serve within the enterprise facility's **102** networked computer-based infrastructure. For instance, computer support components provided as hubs **148**, routers, server facility **142**, firewalls **138**, and the like, may require unique security application software to protect their portion of the system infrastructure, while providing an element in an integrated threat management system that extends out beyond the threat management facility **100** to incorporate all computer resources under its protection.

The enterprise facility **102** may include a plurality of client facility **144** computing platforms on which the end-point computer security facility **152** is adapted. A client facility **144** computing platform may be a computer system that is able to access a service on another computer, such as a server facility **142**, via a network. This client facility **144** server facility **142** model may apply to a plurality of networked applications, such as a client facility **144** connecting to an enterprise facility **102** application server facility **142**, a web browser client facility **144** connecting to a web server facility **142**, an e-mail client facility **144** retrieving e-mail from an internet **154** service provider's mail storage servers **142**, and the like. In embodiments, traditional large client facility **144** applications may be switched to websites, which may increase the browser's role as a client facility **144**. Clients **144** may be classified as a function of the extent to which they perform their own processing. For instance, client facilities **144** are sometimes classified as a fat client facility **144** or thin client facility **144**. The fat client facility **144**, also known as a thick client facility **144** or rich client facility **144**, may be a client facility **144** that performs the bulk of data processing operations itself, and does not necessarily rely on the server facility **142**. The fat client facility **144** may be most common in the

form of a personal computer, where the personal computer may operate independent of any server facility **142**. Programming environments for fat clients **144** may include Curl, Delphi, Droplets, Java, win32, X11, and the like. Thin clients **144** may offer minimal processing capabilities, for instance, the thin client facility **144** may primarily provide a graphical user interface provided by an application server facility **142**, which may perform the bulk of any required data processing. Programming environments for thin clients **144** may include JavaScript/AJAX, ASP, JSP, Ruby on Rails, Python's Django, PHP, and the like. The client facility **144** may also be a mix of the two, such as processing data locally, but relying on a server facility **142** for data storage. As a result, this hybrid client facility **144** may provide benefits from both the fat client facility **144** type, such as multimedia support and high performance, and the thin client facility **144** type, such as high manageability and flexibility. In embodiments, the threat management facility **100**, and associated end-point computer security facility **152**, may provide seamless threat protection to the plurality of clients **144**, and client facility **144** types, across the enterprise facility **102**.

The enterprise facility **102** may include a plurality of server facility **142**, such as application servers **142**, communications servers **142**, file servers **142**, database servers **142**, proxy servers **142**, mail servers **142**, fax servers **142**, game servers **142**, web servers **142**, and the like. A server facility **142**, which may also be referred to as a server facility **142** application, server facility **142** operating system, server facility **142** computer, or the like, may be an application program or operating system that accepts client facility **144** connections in order to service requests from clients **144**. The server facility **142** application may run on the same computer as the client facility **144** using it, or the server facility **142** and the client facility **144** may be running on different computers and communicating across the network. Server facility **142** applications may be divided among server facility **142** computers, with the dividing depending upon the workload. For instance, under light load conditions all server facility **142** applications may run on a single computer and under heavy load conditions a single server facility **142** application may run on multiple computers. In embodiments, the threat management facility **100** may provide threat protection to server facilities **142** within the enterprise facility **102** as load conditions and application changes are made.

A server facility **142** may also be an appliance facility **140**, where the appliance facility **140** provides specific services onto the network. Though the appliance facility **140** is a server facility **142** computer, that may be loaded with a server facility **142** operating system and server facility **142** application, the enterprise facility **102** user may not need to configure it, as the configuration may have been performed by a third party. In an embodiment, an enterprise facility **102** appliance may be a server facility **142** appliance that has been configured and adapted for use with the threat management facility **100**, and located within the facilities of the enterprise facility **102**. The enterprise facility's **102** threat management appliance may enable the enterprise facility **102** to administer an on-site local managed threat protection configuration, where the administration facility **134** may access the threat resources through an interface, such as a web portal. In an alternate embodiment, the enterprise facility **102** may be managed remotely from a third party, vendor, or the like, without an appliance facility **140** located within the enterprise facility **102**. In this instance, the appliance functionality may be a shared hardware product between pluralities of enterprises **102**. In embodiments, the appliance facility **140** may be located at the enterprise facility **102**, where the enterprise facility **102** maintains a degree of control. In embodiments, a hosted service may be provided, where the appliance **140** may still be an on-site black box to the enterprise facility **102**, physically placed there because of infrastructure requirements, but managed by a third party, vendor, or the like.

Simple server facility **142** appliances may also be utilized across the enterprise facility's **102** network infrastructure, such as switches, routers, wireless routers, hubs **148**, gateways, print servers **142**, net modems, and the like. These simple server facility appliances may not require configuration by the enterprise facility **102**, but may require protection from threats via an end-point computer security facility **152**. These appliances may provide interconnection services within the enterprise facility **102** network, and therefore may advance the spread of a threat if not properly protected.

One way for a client facility **144** to be protected from threats from within the enterprise facility **102** network may be a personal firewall. A personal firewall may be an application that controls network traffic to and from a client, permitting or denying communications based on a security policy. Personal firewalls may be designed for use by end-users, which may result in protection for only the computer on which it's installed. Personal firewalls may be able to control network traffic by providing prompts each time a connection is attempted and adapting security policy accordingly. Personal firewalls may also provide some level of intrusion detection, which may allow the software to terminate or block connectivity where it suspects an intrusion is being attempted. Other features that may be provided by a personal firewall may include alerts about outgoing connection attempts, control of program access to networks, hiding the client from port scans by not responding to unsolicited network traffic, monitoring of applications that may be listening for incoming connections, monitoring and regulation of incoming and outgoing network traffic, prevention of unwanted network traffic from installed applications, reporting applications that make connection attempts, reporting destination servers with which applications may be attempting communications, and the like. In embodiments, the personal firewall may be provided by the treat management facility **100**.

Another important component that may be protected by an end-point computer security facility **152** is a network firewall facility **138**, which may be a hardware or software device that may be configured to permit, deny, or proxy data through a computer network that has different levels of trust in its source of data. For instance, an internal enterprise facility **102** network may have a high level of trust, because the source of all data has been sourced from within the enterprise facility **102**. An example of a low level of trust is the Internet **154**, because the source of data may be unknown. A zone with an intermediate trust level, situated between the Internet **154** and a trusted internal network, may be referred to as a "perimeter network". Since firewall facilities **138** represent boundaries between threat levels, the end-point computer security facility **152** associated with the firewall facility **138** may provide resources that may control the flow of threats at this enterprise facility **102** network entry point. Firewall facilities **138**, and associated end-point computer security facility **152**, may also be associated with a network node that may be equipped for interfacing between networks that use different protocols. In embodiments, the end-point computer security facility **152** may provide threat protection in a plurality of network infrastructure locations, such as at the enterprise facility **102** network entry point, i.e. the firewall facility **138** or gateway; at the server facility **142**; at distribution points within the network, i.e. the routers and hubs **148**; at the desktop of client facility **144** computers; and the like. In embodiments, the

most effective location for threat detection may be at the user's computer desktop end-point computer security facility **152**.

The interface between the threat management facility **100** and the enterprise facility **102**, and through the appliance facility **140** to embedded end-point computer security facilities, may include a set of tools that may be the same for all enterprise implementations, but allow each enterprise to implement different controls. In embodiments, these controls may include both automatic actions and managed actions. Automatic actions may include downloads of the end-point computer security facility **152** to components of the enterprise facility **102**, downloads of updates to existing end-point computer security facilities of the enterprise facility **102**, uploaded network interaction requests from enterprise facility **102** components to the threat management facility **100**, and the like. In embodiments, automatic interactions between the enterprise facility **102** and the threat management facility **100** may be configured by the threat management facility **100** and an administration facility **134** in the enterprise facility **102**. The administration facility **134** may configure policy rules that determine interactions, such as developing rules for accessing applications, as in who is authorized and when applications may be used; establishing rules for ethical behavior and activities; rules governing the use of entertainment software such as games, or personal use software such as IM **162** and VoIP **164**; rules for determining access to enterprise facility **102** computing resources, including authentication, levels of access, risk assessment, and usage history tracking; rules for when an action is not allowed, such as whether an action is completely deigned or just modified in its execution; and the like. The administration facility **134** may also establish license management, which in turn may further determine interactions associated with a licensed application. In embodiments, interactions between the threat management facility **100** and the enterprise facility **102** may provide threat protection to the enterprise facility **102** by managing the flow of network data into and out of the enterprise facility **102** through automatic actions that may be configured by the threat management facility **100** or the administration facility **134**.

Client facilities **144** within the enterprise facility **102** may be connected to the enterprise facility **102** network by way of wired network facilities **148** or wireless network facilities **150**. Client facilities **144** connected to the enterprise facility **102** network via a wired facility **148** or wireless facility **150** may receive similar protection, as both connection types are ultimately connected to the same enterprise facility **102** network, with the same end-point computer security facility **152**, and the same threat protected enterprise facility **102** environment. Mobile wireless facility **150** clients **144**, because of their ability to connect to any wireless **150** network access point, may connect to the internet **154** outside the enterprise facility **102**, and therefore outside the threat-protected environment of the enterprise facility **102**. In this instance the mobile client facility **144**, if not for the presence of the end-point computer security facility **152** may experience a malware attack or perform actions counter to enterprise facility **102** established policies. In addition, there may be a plurality of ways for the threat management facility **100** to protect the out-of-enterprise facility **102** mobile client facility **144** that has an embedded end-point computer security facility **152**, such as by providing URL filtering in personal routers, using a web appliance as a DNS proxy, or the like. Mobile client facilities **144** that are components of the enterprise facility **102** but temporarily outside connectivity with the enterprise facility **102** network, may be provided with the same threat protection and policy control as client facilities **144** inside the enterprise facility **102**. In addition, mobile client facilities **144** may receive the same interactions to and from the threat management facility **100** as client facilities **144** inside the enterprise facility **102**, where mobile client facilities **144** may be considered a virtual extension of the enterprise facility **102**, receiving all the same services via their embedded end-point computer security facility **152**.

Interactions between the threat management facility **100** and the components of the enterprise facility **102**, including mobile client facility **144** extensions of the enterprise facility **102**, may ultimately be connected through the internet **154**. Threat management facility **100** downloads and upgrades to the enterprise facility **102** may be passed from the firewalled networks of the threat management facility **100** through to the end-point computer security facility **152** equipped components of the enterprise facility **102**. In turn the end-point computer security facility **152** components of the enterprise facility **102** may upload policy and access requests back across the internet **154** and through to the threat management facility **100**. The Internet **154** however, is also the path through which threats may be transmitted from their source. These network threats may include threats from a plurality of sources, including websites **158**, e-mail **160**, IM **162**, VoIP **164**, application software, and the like. These threats may attempt to attack a mobile enterprise facility **102** client facility **144** equipped with an end-point computer security facility **152**, but in embodiments, as long as the mobile client facility **144** is embedded with an end-point computer security facility **152**, as described above, threats may have no better success than if the mobile client facility **144** where inside the enterprise facility **102**.

However, if the mobile client facility **144** where to attempt to connect into an unprotected connection point, such as at a secondary location **108** that is not a part of the enterprise facility **102**, the mobile client facility **144** may be required to request network interactions through the threat management facility **100**, where contacting the threat management facility **100** may be performed prior to any other network action. In embodiments, the client facility's **144** end-point computer security facility **152** may manage actions in unprotected network environments such as when the client facility **144** is in a secondary location **108** or connecting wirelessly **150** to a non-enterprise facility **102** wireless internet **154** connection, where the end-point computer security facility **152** may dictate what actions are allowed, blocked, modified, or the like. For instance, if the client facility's **144** end-point computer security facility **152** is unable to establish a secured connection to the threat management facility **100**, the end-point computer security facility **152** may inform the user of such, and recommend that the connection not be made. In the instance when the user chooses to connect despite the recommendation, the end-point computer security facility **152** may perform specific actions during or after the unprotected connection is made, including running scans during the connection period, running scans after the connection is terminated, storing interactions for subsequent threat and policy evaluation, contacting the threat management facility **100** upon first instance of a secured connection for further actions and or scanning restricting access to network and local resources, or the like. In embodiments, the end-point computer security facility **152** may perform specific actions to remediate possible threat incursions or policy violations during or after the unprotected connection.

The secondary location **108** may have no end-point computer security facilities **152** as a part of its computer components, such as its firewalls **138**, servers **142**, clients **144**, hubs

148, wireless hubs 150, and the like. As a result, the computer components of the secondary location 108 may be open to threat attacks, and become potential sources of threats, as well as any mobile enterprise facility 102 clients 144 that may be connected to the secondary location's 108 network. In this instance, these computer components may now unknowingly spread a threat to other components connected to the network.

Some threats may not come directly from the Internet 154, such as from non-enterprise facility 102 controlled mobile devices that are physically brought into the enterprise facility 102 and connected to the enterprise facility 102 client facilities 144. The connection may be made from direct connection with the enterprise facility's 102 client facility 144, such as through a USB port, or in physical proximity with the enterprise facility's 102 client facility 144 such that a wireless facility 150 connection can be established, such as through a Bluetooth connection. These physical proximity threats 110 may be another mobile computing device, a portable memory storage device, a mobile communications device, or the like, such as CDs and DVDs 170, memory stick 174, flash drive 174, external hard drive, cell phone 178, PDAs 180, MP3 players, digital cameras, point-to-point devices, or the like. A physical proximity threat 110 may have been previously infiltrated by network threats while connected to an unprotected network connection outside the enterprise facility 102, and when connected to the enterprise facility 102 client facility 144, pose a threat. Because of their mobile nature, physical proximity threats 110 may infiltrate computing resources in any location, such as being physically brought into the enterprise facility 102 site, connected to an enterprise facility 102 client facility 144 while that client facility 144 is mobile, plugged into an unprotected client facility 144 at a secondary location 108, and the like. A mobile device, once connected to an unprotected computer resource, may become a physical proximity threat 110. In embodiments, the end-point computer security facility 152 may provide enterprise facility 102 computing resources with threat protection against physical proximity threats 110, for instance, through scanning the device prior to allowing data transfers, through security validation certificates, through establishing a safe zone within the enterprise facility 102 computing resource to transfer data into for evaluation, and the like.

Now that the overall system has been described, we turn towards a set of dynamic internet address assignment embodiments, where the assignment may be based on user identity and policy compliance. It should be understood that the following embodiments may be managed through a threat management facility 100 along with other services, such as those described herein.

In embodiments, the client 144 when connecting to a network, requests an internet protocol (IP) address from a dynamic host configuration protocol (DHCP) server 204. The responding DHCP server 204 may then assign an IP address to the client. The DHCP server 204 may also assign DHCP options to the client 144 that are necessary for the client 144 to operate on an IP network. The present invention may then intercept the assignment process, and intervene with the DHCP server 204 prior to the initially assigned IP address and the DHCP options being transmitted back to the client 144. This may be done in order to provide the opportunity to change the IP assignment and/or the DHCP options based on a policy, where the change may be based on user identity, policy compliance, and the like. Through the present invention, the network administrator 134 may be provided better control over the use and access of clients 144 and users to the network through a policy management facility 112. The present invention may thus increase the security of the network.

In embodiments, the present invention may facilitate the interception of the IP assignment process through software placed on the DHCP server 204A, often referred to as a software plug-in 208. This DHCP plug-in 208 may provide both a mechanism for interrupting the transmission of initially assigned IP address and DHCP options, and for a communications interface to the policy management facility 112. In embodiments, this communications interface may be made directly or indirectly, such as through a server 142, applications server 210, and the like. Through this interface, the DHCP plug-in 208 may provide client information to the policy management facility 134 that was gathered by the DHCP server 204 during the period when the client 144 was making the IP assignment request. Client information, such as information related to the user, compliance status, client configuration, and the like, may then be utilized by the policy management facility 112 to determine what network access parameters to grant to the client 144. In embodiments, the granting of network access parameters to the client 144, or the restriction thereof, may be provided through a selection of IP address and/or DHCP options, which when selected by the policy management facility 112 may be communicated back to the DHCP plug-in 208. Finally, the DHCP plug-in 208 may provide the new IP address and/or DHCP options to the DHCP server 204A, which may then change the initially assigned client IP address and/or DHCP options, to the new client IP address and/or DHCP options for transmission to the client 144. In embodiments, the changes may be only to the DHCP options, only to the IP address, to both the IP address and DHCP options, and the like. In embodiments, the changes to an IP address or DHCP option may be made by the DHCP plug-in 208 or DHCP server 204A as a result of communications from the policy management facility 112.

In embodiments, the client 144 may receive an IP address and DHCP options that may restrict a user's access to the network. For instance, the client user may be listed as part of an engineering department, and as a result their network access may be determined by what policy dictates access is to be for the engineering department, such as to engineering applications, engineering databases, technical search engines, design tools, and the like. Or, the client user may be listed as a part of a human resources department, and as a result their network access may be determined by what policy dictates access is to be for the human resources department, such as to personnel files, appraisal files, facility access lists, and the like. In another instance, the client user may be a top executive of the company, and as a result their network access may provide for open access to all network resources.

In embodiments, the client 144 may receive an IP address and DHCP options that may restrict the client 144 access to the network. For instance, the client 144 may be determined to be out of compliance with respect to the software licenses on the client 144, malware protection software, updates to software, and the like. If the client 144 is determined to be out of compliance, the IP address and DHCP options may be related to restricted network access, such as being in quarantine, restricted to only external access, disconnected from the network, and the like. In embodiments, if the client 144 is found to be within compliance, the client 144 may receive an IP address and DHCP options that provide normal network access relative to their user access privileges.

In embodiments, the present invention may provide for a more secure network environment due the control of client

network access enabled through established policies within the policy management facility **112**.

Referring to FIG. **2** a process flow embodiment is shown for dynamic internet address assignment based on user identity and policy compliance. While describing FIG. **2**, references may be made to FIG. **1**. Further, those skilled in the art would appreciate that the process flow of FIG. **2** may be implemented in any other environment apart from FIG. **1**. Further, it may be noted that the process flow may include some or all process blocks as shown in FIG. **2**.

Referring to FIG. **2**, at step **1**, the client **144** may request an IP address from a DHCP server **204**A. The client **144** may provide client information **202** to the DHCP server **204**A. The client may include client information **202** and the security facility **152**. Further it should be noted that a single client **144** is shown in FIG. **2**. However, those skilled in the art would appreciate that one or more clients may be present.

In embodiments, the client request may be made when the client **144** initializes the network. The network may be a wired or wireless. In embodiments, the client **144** may request an IP address from the DHCP server **204**A when connecting to the network for a first time. In embodiments, the client **144** may request the IP address from the DHCP server **204**A during boot up. In embodiments, the client request may be made in association with a lease. In embodiment, the client request may be generated through a TCP/IP configured software resident on the client **144**. In embodiments, the client request for the IP address may be made in association with a security threat detected by the client end-point security facility **152**.

In embodiments, the DHCP server **204**A may implement a protocol. The protocol may be used by the client **144** to obtain parameters necessary for the client **144** to operate on an internet protocol (IP) network. Further, in embodiments, the parameter may be an IP address, a subnet mask, a default gateway, a lease, a TCP/IP configuration parameter, or some other type of parameter. In embodiments, the lease may be associated with the length of time for which an IP address may be allocated. Further, the lease may be renewed.

In embodiments, the client **144** may send a broadcast query on the network **154** requesting for parameters from the DHCP server **204**A. In embodiments, the broadcast query may be associated with discovery about the available DHCP servers including the DHCP server **204**A on the physical subnet. For example, the broadcast query may discover the DHCP server **204**A or the DHCP server **204**B. In embodiments, the client **144** may send the broadcast query when the client **144** performs network initialization. In embodiments, the client **144** may send the broadcast query when the client **144** boots up.

In embodiments, the DHCP server **204**A may provide a dynamic allocation of the IP addresses. Further, the dynamic allocation may provide a range of IP addresses. The range of IP addresses may be assigned by the administrator **134**. For example, the DHCP server **204**A may provide IP addresses ranging from 202.12.12.100 to 202.12.12.176 that may be assigned by the network administrator. In embodiments, the dynamic allocation may utilize the lease. The lease may represent the time period for which the IP address may be valid.

In embodiments, the DHCP server **204**A may manage multiple IP addresses. The IP addresses that may be managed by the DHCP server may be allocated. The allocation may be made by an internet assigned numbers authority. In embodiments, the allocation of IP address may be by a regional internet registry. In embodiments, the allocation of IP address may be by an enterprise administrator.

In embodiments, a unique IP address may be assigned to the network components of an IP network. For example, the client **144**A may be allocated an IP address 202.123.11.110 the client **144**B may be allocated IP address 202.123.11.111 and the like. The unique IP addresses assigned to the client **144**A and the client **144**B may enable the client **144**A and the client **144**B to communicate with each other. Further, those skilled in the art would appreciate that other network components may be assigned IP address that would be unique in the network and may allow them to communicate with other network components in the network. In embodiments, the IP address may be a unique IP address on the internet **154**. In embodiments, the IP address may be for a specific network. For example, the unique IP may be for a LAN network. In embodiments, the IP address may be unique for an enterprise **102**. In embodiments, the IP address may be private.

In embodiments, the client **144** may provide the client information **202** along with the request for an IP address to the DHCP server **204**A. In embodiments, the client information **202** may be automatically provided to the DHCP server **204**A along with client request for IP address. In embodiments, the client information **202** may be provided to the DHCP server **204**A on request. Further, the DHCP server **204**A may request for client information **202** whenever the request for IP address is made by the client **144**. In embodiments, the client information **202** request may be made by the DHCP server **204**A in association with the DHCP plug-in **208**. In embodiments, the client information request may be made whenever the DHCP server request may be initiated by the DHCP-plug-in **208**.

In embodiments, the client information **202** may be a MAC address, a time of day, a current location of the client, a user ID, a user name, an IP address requested by the client, a DHCP option requested by the client, a client capability, or some other type of client information. In embodiments, the client capability may be due to presence of a software application. In embodiments, the client capability may be a network access control capability.

In embodiments, the client information **202** may be associated with security vulnerability. In embodiments, the security vulnerability may be associated with malware security venerability. Further, the malware security vulnerability may be associated with the client **144** having no end-point security facility **152**. The end-point computer security facility **152** may be the malware security software.

In embodiments, the malware security vulnerability may be associated with the client **144** having out of date end-point computer security facility **152**. In embodiments, the malware security vulnerability may be associated with the client end-point security facility **152** that may detect a malware threat. In embodiments, the malware security vulnerability may be from the client end-point security facility **152** that may detect suspicious behavior.

In embodiments, the security vulnerability may be associated with a client end-point firewall. In embodiments, there may not be any client end-point firewall. In embodiments, the client end-point firewall may be improperly configured.

In embodiments, the client information may be software vulnerability. Further, the software vulnerability may be associated with a license. The license may be out of date. In embodiments, there may be no valid license agreement available with the client **144**.

In embodiments, the software vulnerability may be associated with a registration. Further, the registration may be out of date. In embodiments, the registration may not be a valid registration. In embodiments, the software vulnerability may be an unauthorized software application that may be associated with the client **144**.

In embodiments, the client information **202** may be a client configuration status. The client information status may be associated with the policy management facility **112**. The policy management facility **112** may read the configuration status as an indication of policy compliance. In embodiments, the client information status may be associated with the client operating system. In embodiments, the client information status may be associated with the client end point security facility **152**.

Referring to the process flow of FIG. **2** at step **2** a first IP assignment and a first multiple DHCP options may be formulated at the DHCP server **204**A.

In embodiments, the multiple DHCP options associated with DHCP server **204**A may be used to assign network configuration parameters. The configuration may be automatic. In embodiments, the configuration may be for IP hosts. In embodiments, the network configuration parameter may be associated with full network access. In embodiments, the network configuration parameter may be associated with normal network access. In embodiments, the network configuration parameter may be associated with restricted access. The restricted access may provide external network access including an access to internet **154**. In embodiments, the network configuration parameter may be associated with isolating the client **144**A from client **144**B. The isolated client **144**A may be associated with quarantine.

In embodiments, the network configuration parameter may be a subnet mask, a router, a time server, a name server, a domain server, a log server, a quotes server, a LPR server, an impress server, a RLP server, a hostname, a domain name, a static route, a vendor specific, an address request, an address time, a class ID, a client ID, a relay agent information, a classless static route, an IEE 802.1Q VLAN ID, or some other type of network configuration parameters.

Referring to the process flow of FIG. **2** at step **3**. The DHCP plug-in **208** may intercept the first IP assignment and the multiple DHCP options. The DHCP plug-in **208** may be provided in the DHCP server **204**A. The DHCP plug-in **208** may act as an application server client to an application server **210**A. As result of the interception, the process flow of FIG. **2** may stop the sending of information relating to the first IP assignment and the multiple DHCP options to the client **144**.

In embodiments, the interception may be provided by the DHCP plug-in **208**. In embodiments, the interception may be provided by the application server **210**. In embodiments, the interception may be provided by the policy management facility **112**.

Referring to the process flow of FIG. **2** at step **4**, the DHCP plug-in **208** may send the client information to the application server **210**.

Referring to the process flow of FIG. **2**, at step **5**, the application server **210** may send the client information to the policy management facility **112**. The policy management facility **112** may formulate a second multiple DHCP options in association with policy associated with the enterprise **102**.

In embodiments, the formulation of the second multiple DHCP options may be in association with the policy management facility **112**. The policy management facility **112** may be associated with a policy. The policy may be associated with a user identification. For example, when a user is identified as an administrator of the network a super user policy may be implemented. The user identification may be associated with an enterprise organization set of policies for the enterprise **102**. In embodiments, the enterprise organizational set of policies may be associated with a department. In embodiments, the enterprise organizational set of policies may be associated with a management position within the enterprise. In embodiments, the enterprise organizational set of policies may be associated with a personnel position within the enterprise. In embodiments, the enterprise organizational set of policies may be associated with an outside contractor. In embodiments, the enterprise organizational set of policies may be associated with a visitor to the enterprise.

In embodiments, the user identification may be associated with employment status. In embodiment, the user identification may be associated with personal policy profile.

In embodiments, the profile may be associated with the client configuration. The client configuration may be associated with compliance. Further, the compliance may be end-point security compliance. Furthermore, the end-point security may be associated with client **144** that may have updated end-point security software **152**.

In embodiments, the compliance may be a software application compliance, a hardware compliance, a registration compliance, a license compliance, or some other type of compliance.

In embodiments, the client configuration may be associated with a client capability. The client capability may be a software capability, a hardware capability, a network access capability, an interface capability, or some other type of client capability.

In embodiments, the policy may be associated with an end-point security status. The end-point security status may indicate detection of malware. In embodiments, the end point security status may indicate a detection of suspicious behavior. The suspicious behavior may be associated with a software file. In embodiments, the suspicious behavior may be associated with a user action.

In embodiments, the policy may be associated with a location. In embodiments, the location may be a current location, a geographic location, a personal location, mobile location, an enterprise location, or some other type of location. In embodiments the location may be associated with the home location, the previous location, or some other type of location.

In embodiments, the policy may be associated with time. The time may be associated with work hours. In embodiments, the time may normal working hours, after working hours, late night, or some other time.

Referring to the process flow of FIG. **2** at step **6**, the formulated second multiple DHCP options may be sent from the policy management facility **112** to the application server **210**. In embodiments, the formulated second multiple DHCP options may be sent directly to the DHCP plug-in **208**, or directly to the DHCP server **204**.

Referring to the process flow of FIG. **2** at step **7** the application server **210** may send the formulated multiple DHCP options information to DHCP plug-in. **208**.

Referring to the process flow of FIG. **2** at step **8**, the formulated multiple DHCP options received by the DHCP plug-in. **208** may be implemented on the DHCP server **204**A. The DHCP server **204**A may change the DHCP options from the first IP assignment and first multiple DHCP options to the second IP assignment and the second multiple DHCP options in association with DHCP plug-in **208**.

Referring to the process flow of FIG. **2** at step **9**, the DHCP server **204**A may send the second IP assignment and the second multiple DHCP options to the client **144**. The client **144** may apply the second IP assignment and the second multiple DHCP options in association with the client security facility **152**.

Referring to the process flow of FIG. **2** at step **10**, the client **144** may communicate with the application server **210**.

Referring to FIG. **3**, a process **300** is illustrated. The process **300** starts at logical block **302**. At logical block **302** the

client **144** may be presented. The client **144** may request an IP address from the DHCP server **204**A. In addition, the client **144** may provide client information to the DHCP server **204**A.

At logical block **304**, the DHCP server **204**A may formulate a first IP assignment and a first multiple DHCP options. At logical block **308**, the policy management facility **112** may intercept the first IP assignment and the first multiple DHCP options. As a result of interception by the policy management facility **112**, the DHCP server **204**A may stop the sending of the first IP assignment and the first multiple DHCP option to the client **144**.

At logical block **310**, the client information may be sent from the DHCP server **204**A to the policy management facility **112**.

At logical block **312**, a second set of multiple DHCP options may be formulated. The formulation of the second multiple DHCP options may be in association with policy management facility **112**. The second multiple DHCP options may be sent from the policy management facility **112** to the DHCP server **204**A.

At logical block **314**, the DHCP server **204**A may change the first IP assignment and the first multiple DHCP options to the second IP assignment and the second multiple DHCP options.

At logical block **318**, the DHCP server **204**A may send the second IP assignment and the second multiple DHCP options to the client **144**. The client **144** may apply the second IP assignment and the second multiple DHCP options in association with a client security facility **152**.

Referring to FIG. **4**, a process **400** is illustrated. The process **400** starts at logical block **402**. At logical block **402** a client **144** may be presented. The client **144** may request an IP address from the DHCP server **204**A. In addition, the client **144** may provide client information to the DHCP server **204**A.

At logical block **404**, the DHCP server **204**A may formulate a first IP assignment and a first multiple DHCP options. At logical block **408**, a DHCP plug-in **208** may be provided in the DHCP server **204**A. At logical block **410**, the DHCP plug-in **208** may intercept the first IP assignment and the first multiple DHCP options. The interception by the DHCP plug-in **208** may stop the sending of the first IP assignment and the first multiple DHCP options to the client **144**.

At logical block **412**, the client information may be sent to the policy management facility **112** through the DHCP-plug-in **208**.

At logical block **414**, a second multiple DHCP options may be formulated. The formulation of the second multiple DHCP options may be in association with policy management facility **112**. Further, the second multiple DHCP options may be sent from the policy management facility **112** to the DHCP plug-in **208**.

At logical block **418**, the DHCP server **204**A may change the first IP assignment and the first multiple DHCP options to the second IP assignment and the second multiple DHCP options. In addition the changing of options from the first IP assignment and the first multiple DHCP options to the second IP assignment and the second multiple DHCP options may be in association with the DHCP plug-in **208**.

At logical block **420**, the DHCP server **204**A may send the second IP assignment and the second multiple DHCP options to the client **144**. The client **144** may apply the second IP assignment and the second multiple DHCP options in association with a client security facility **152**.

Referring to FIG. **5**, a process **500** is illustrated. The process **500** starts at logical block **502**. At logical block **502** a client **144** may be presented. The client **144** may request an IP address from the DHCP server **204**A. In addition, the client **144** may provide client information to the DHCP server **204**A.

At logical block **504**, the DHCP server **204**A may formulate a first IP assignment and a first multiple DHCP options. At logical block **508**, a DHCP plug-in **208** may be provided in the DHCP server **204**A. At logical block **510**, the DHCP plug-in **208** may intercept the first IP assignment and the first multiple DHCP options. The interception by the DHCP plug-in **208** may stop the sending of the first IP assignment and the first multiple DHCP options to the client **144**.

At logical block **512**, the client information may be sent from the DHCP plug-in **208** to the application server **210**.

At logical block **514**, the client information may be sent from the application server **210** to the policy management facility **112**.

At logical block **518**, a second multiple DHCP options may be formulated. The formulation of the second multiple DHCP options may be in association with policy management facility **112**. Further, the second multiple DHCP options may be sent from the policy management facility **112** to the DHCP plug-in **208** through the application server **210**.

At logical block **520**, the DHCP server **204**A may change the first IP assignment and the first multiple DHCP options to a second IP assignment and the second multiple DHCP options. In addition the changing of options from the first IP assignment and the first multiple DHCP options to the second IP assignment and the second multiple DHCP options may be in association with the DHCP plug-in **208**.

At logical block **522**, the DHCP server **204**A may send the second IP assignment and the second multiple DHCP options to the client **144**. The client **144** may apply the second IP assignment and the second multiple DHCP options in association with a client security facility **152**.

The elements depicted in flow charts and block diagrams throughout the figures imply logical boundaries between the elements. However, according to software or hardware engineering practices, the depicted elements and the functions thereof may be implemented as parts of a monolithic software structure, as standalone software modules, or as modules that employ external routines, code, services, and so forth, or any combination of these, and all such implementations are within the scope of the present disclosure. Thus, while the foregoing drawings and description set forth functional aspects of the disclosed systems, no particular arrangement of software for implementing these functional aspects should be inferred from these descriptions unless explicitly stated or otherwise clear from the context.

Similarly, it will be appreciated that the various steps identified and described above may be varied, and that the order of steps may be adapted to particular applications of the techniques disclosed herein. All such variations and modifications are intended to fall within the scope of this disclosure. As such, the depiction and/or description of an order for various steps should not be understood to require a particular order of execution for those steps, unless required by a particular application, or explicitly stated or otherwise clear from the context.

The methods or processes described above, and steps thereof, may be realized in hardware, software, or any combination of these suitable for a particular application. The hardware may include a general-purpose computer and/or dedicated computing device. The processes may be realized in one or more microprocessors, microcontrollers, embedded microcontrollers, programmable digital signal processors or other programmable device, along with internal and/or exter-

nal memory. The processes may also, or instead, be embodied in an application specific integrated circuit, a programmable gate array, programmable array logic, or any other device or combination of devices that may be configured to process electronic signals. It will further be appreciated that one or more of the processes may be realized as computer executable code created using a structured programming language such as C, an object oriented programming language such as C++, or any other high-level or low-level programming language (including assembly languages, hardware description languages, and database programming languages and technologies) that may be stored, compiled or interpreted to run on one of the above devices, as well as heterogeneous combinations of processors, processor architectures, or combinations of different hardware and software.

Thus, in one aspect, each method described above and combinations thereof may be embodied in computer executable code that, when executing on one or more computing devices, performs the steps thereof. In another aspect, the methods may be embodied in systems that perform the steps thereof, and may be distributed across devices in a number of ways, or all of the functionality may be integrated into a dedicated, standalone device or other hardware. In another aspect, means for performing the steps associated with the processes described above may include any of the hardware and/or software described above. All such permutations and combinations are intended to fall within the scope of the present disclosure.

While the invention has been disclosed in connection with the preferred embodiments shown and described in detail, various modifications and improvements thereon will become readily apparent to those skilled in the art. Accordingly, the spirit and scope of the present invention is not to be limited by the foregoing examples, but is to be understood in the broadest sense allowable by law.

All documents referenced herein are hereby incorporated by reference.

What is claimed is:

1. A method, comprising: presenting a client requesting an IP address from a DHCP server, wherein the client provides client information to the DHCP server; formulating a first IP assignment and a first plurality of DHCP options by the DHCP server;

intercepting the first IP assignment and the first plurality of DHCP options by a policy management facility, wherein intercepting stops the sending of the first IP assignment and the first plurality of DHCP options to the client;

sending client information to the policy management facility;

formulating a second plurality of DHCP options in association with the policy management facility, wherein the second plurality of DHCP options is sent from the policy management facility to the DHCP server;

changing the DHCP options in the DHCP server from the first IP assignment and first plurality of DHCP options to a second IP assignment and the second plurality of DHCP options;

sending the second IP assignment and the second plurality of DHCP options from the DHCP server to the client, wherein the client applies the second IP assignment and the second plurality of DHCP options in association with a client security facility;

wherein the plurality of DHCP options are used to assign network configuration parameters; and

wherein the network configuration parameter is associated with restricted access.

2. The method of claim **1** wherein the network configuration parameter is associated with full network access.

3. The method of claim **1** wherein the network configuration parameter is associated with normal network access.

4. The method of claim **1** wherein the restricted access provides only external network access.

5. The method of claim **1** wherein the network configuration parameter is associated with isolating the client.

6. The method of claim **5** wherein isolating the client is associated with quarantine.

7. The method of claim **1** wherein the network configuration parameter is a subnet mask.

8. The method of claim **1** wherein the network configuration parameter is a router.

9. The method of claim **1** wherein the network configuration parameter is a time server.

10. The method of claim **1** wherein the network configuration parameter is a name server.

11. The method of claim **1** wherein the network configuration parameter is a domain server.

12. The method of claim **1** wherein the network configuration parameter is a log server.

13. The method of claim **1** wherein the network configuration parameter is a quotes server.

14. The method of claim **1** wherein the network configuration parameter is a LPR server.

15. The method of claim **1** wherein the network configuration parameter is an impress server.

16. The method of claim **1** wherein the network configuration parameter is a RLP server.

17. The method of claim **1** wherein the network configuration parameter is a hostname.

18. The method of claim **1** wherein the network configuration parameter is a domain name.

19. The method of claim **1** wherein the network configuration parameter is a static route.

20. The method of claim **1** wherein the network configuration parameter is vendor-specific.

21. The method of claim **1** wherein the network configuration parameter is an address request.

22. The method of claim **1** wherein the network configuration parameter is an address time.

23. The method of claim **1** wherein the network configuration parameter is a class ID.

24. The method of claim **1** wherein the network configuration parameter is a client ID.

25. The method of claim **1** wherein the network configuration parameter is a relay agent information.

26. The method of claim **1** wherein the network configuration parameter is a classless static route.

27. The method of claim **1** wherein the network configuration parameter is an IEEE 802.1Q VLAN ID.

28. The method of claim **1** wherein the client information is provided from the client to the DHCP server.

29. The method of claim **28** wherein the client information is provided by the client as a part of the client request for an IP address.

30. The method of claim **28** wherein the client information is provided automatically as a part of the client request for an IP address.

31. The method of claim **28** wherein the client information is provided when the DHCP server requests the client information.

32. The method of claim **31** where the DHCP server request is in association with a DHCP plug-in.

33. The method of claim **1** wherein the client information is a security vulnerability.

34. The method of claim **33** wherein the security vulnerability is associated with malware security vulnerability.

35. The method of claim **34** wherein the malware security vulnerability is from the client having no end-point security facility.

36. The method of claim **35** wherein the end-point security facility is malware security software.

37. The method of claim **34** wherein the malware security vulnerability is from the client having out of date end-point security facility.

38. The method of claim **34** wherein the malware security vulnerability is from the client security facility detecting a malware threat.

39. The method of claim **34** wherein the malware security vulnerability is from the client security facility detecting suspicious behavior.

40. The method of claim **33** wherein the security vulnerability is associated with a client end-point firewall.

41. The method of claim **40** wherein there is no client end-point firewall.

42. The method of claim **40** wherein the client end-point firewall is improperly configured.

43. The method of claim **1** wherein the client information is a software vulnerability.

44. The method of claim **43** wherein the software vulnerability is an unauthorized software application.

45. The method of claim **1** wherein the client information is a client configuration status.

46. The method of claim **45** wherein the client configuration status is associated with the policy management facility.

47. The method of claim **46** wherein the policy management facility reads the configuration status as an indication of policy compliance.

48. The method of claim **45** wherein the client configuration status is associated with the client operating system.

49. The method of claim **45** wherein the client configuration status is associated with the client security facility.

50. The method of claim **1** wherein intercepting is provided by a DHCP plug-in.

51. The method of claim **1** wherein intercepting is provided by an application server.

52. The method of claim **1** wherein intercepting is provided by the policy management facility.

53. The method of claim **1** wherein the formulating the second plurality of DHCP options in association with the policy management facility is in association with a policy.

54. The method of claim **53** wherein the policy is associated with a user identification.

55. The method of claim **54** wherein the user identification is associated with an enterprise organizational set of policies.

56. The method of claim **55** wherein the enterprise organizational set of policies is associated with a department.

57. The method of claim **55** wherein the enterprise organizational set of policies is associated with an outside contractor.

58. The method of claim **55** wherein the enterprise organizational set of policies is associated with a visitor to the enterprise.

59. The method of claim **53** wherein the policy is associated with a client configuration.

60. The method of claim **59** wherein the client configuration is associated with compliance.

61. The method of claim **59** wherein the client configuration is associated with a client capability.

62. The method of claim **53** wherein the policy is associated with an end-point security status.

63. The method of claim **53** wherein the policy is associated with a location.

64. The method of claim **53** wherein the policy is associated with a time.

* * * * *