

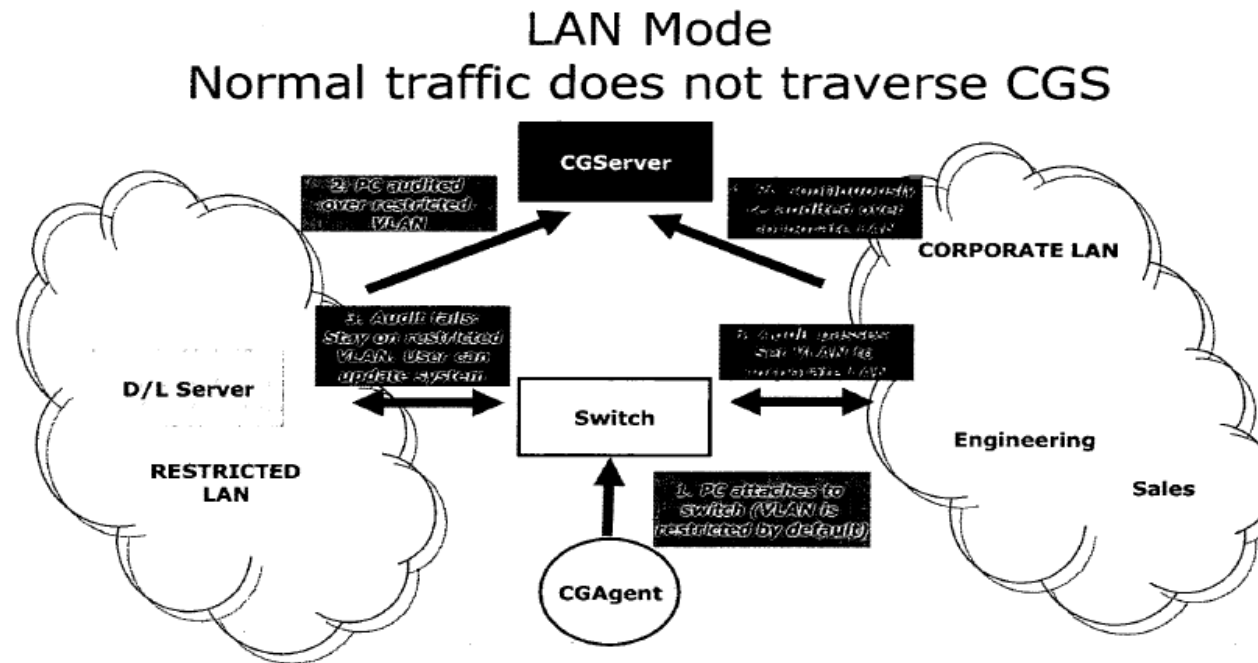
US7523484	Constructive Reduction to Practice (US60/513,080)
[1.0] A network gatekeeper comprising:	Many portions of the '080 provisional specification verify that the invention was directed to the claimed “gatekeeper invention for controlling access to a corporate network and the like. Some examples are the very title itself and the definitions on page 3: <u>Page 3</u> 1 GATEKEEPER INVENTION FOR CONTROLLING ACCESS TO A CORPORATE NETWORK USING 802.1x The invention is directed to controlling access to a corporate network based on audit criteria for end points. The amount of access granted or denied to an end point is determined by policies which specify the audit criteria and types of access. Definitions GK – The software that acts as a gatekeeper by granting or denying access to the corporate network from end points after auditing the end point based on certain criteria.



US7523484	Constructive Reduction to Practice (US60/513,080)
	<u>Page 8</u> Invention According to the invention, an AP may be programmed to prohibit access by the PC to the corporate network until authentication with the authentication server passes AND an audit with the software agent with the GK passes, while still supporting the existing encryption and authentication functionality. The method used to support auditing functionality over the existing 802.1x protocol implementation is complicated and not an obvious variation of the 802.1x protocol. In the invention, the auditing protocol takes place between the EP agent software and the GK. A client filter redirects calls for audit information to an agent on the EP and sends the responses to the 802.1x compliant AP which relays them to the EAP server. The EAP server then calls a server filter which sends the responses to the GK for evaluation. The GK sends requests for more information on the reverse path and this continues until the audit is completed. If the audit is successful, the server sends a message to the AP which enables the EP's port allowing access for the PC. If the audit fails, the port on the AP is left disabled.

US7523484	Constructive Reduction to Practice (US60/513,080)
[1.1] at least one security policy including requirements that must be satisfied before an access device is granted access to a less-restricted subset of a protected network;	The '080 provisional provides a security policy, including requirements that must be satisfied before a device is granted access to a less-restricted subset of a protected network. For example, page 3 provides that “access to a corporate network” is “granted or denied to an end point,” which is a PC or network device (ND), as “determined by [security] policies which specify the audit criteria and types of access.” This access may include access to a less-restricted subset of the network (e.g. the corporate network/LAN). <u>Page 3</u> 1 GATEKEEPER INVENTION FOR CONTROLLING ACCESS TO A CORPORATE NETWORK USING 802.1x The invention is directed to controlling access to a corporate network based on audit criteria for end points. The amount of access granted or denied to an end point is determined by policies which specify the audit criteria and types of access. Definitions GK – The software that acts as a gatekeeper by granting or denying access to the corporate network from end points after auditing the end point based on certain criteria. PC – A notebook, desktop PC, PDA, or similar computing device. ND –Network device such as a network printer, which is normally incapable of running an agent. EP – End point which can be a PC or ND.

Page 19 (note in the figure below the GK (gatekeeper) is referred to as the CGServer)



(c) 2003 InfoExpress, Inc.

4

Page 8 also supports this element, which states “[i]f the audit is successful, the server sends a message to the AP which enables the EP’s port allowing access for the PC. . . .” which “allow[s] access to the less restricted subset of the network.” To access the corporate network, the device must pass both a security policy including an audit. (“an AP may be programmed to prohibit access... until an audit with the software agent with the GK passes...”).

Page 8

Invention

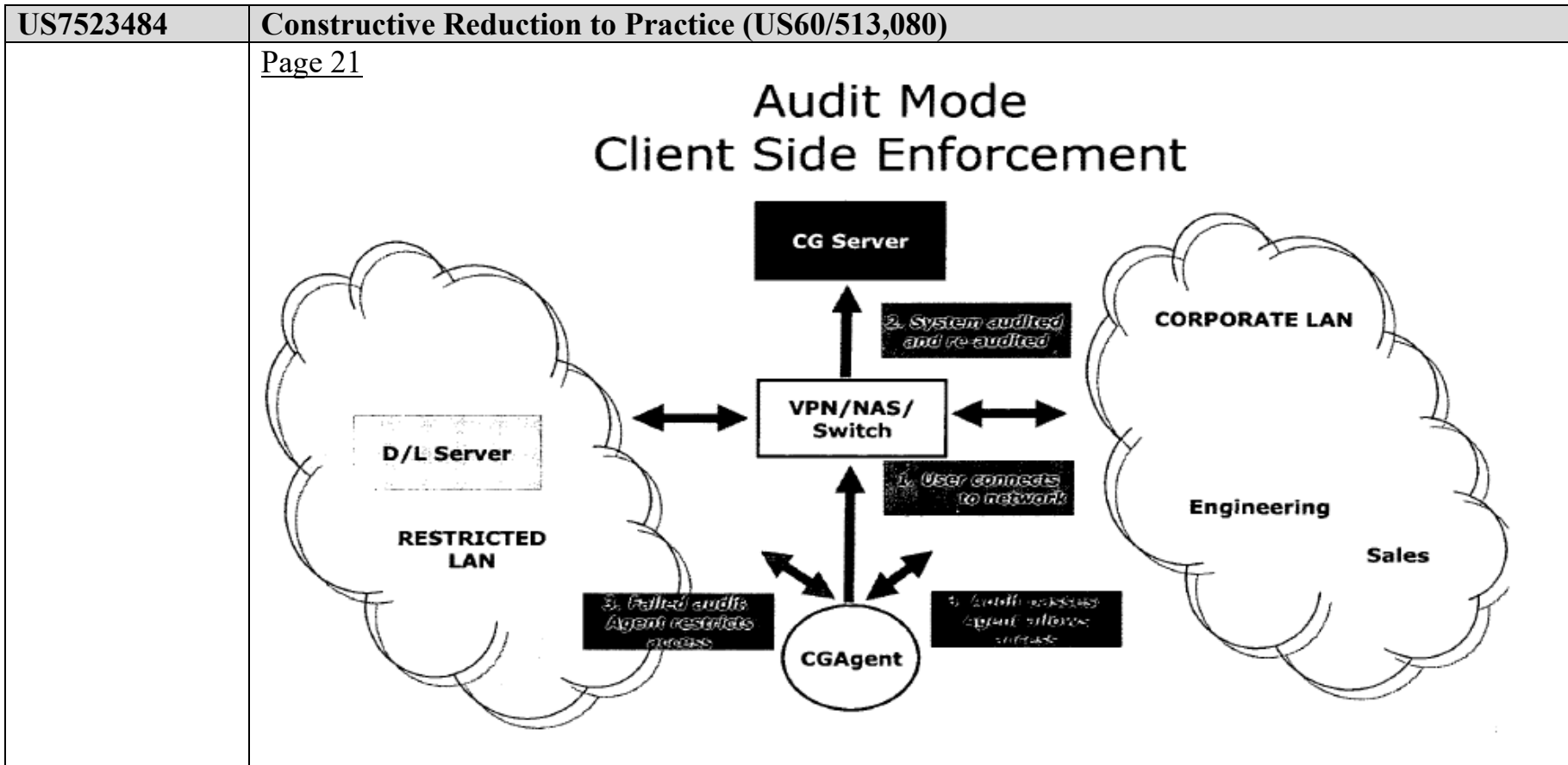
According to the invention, an AP may be programmed to prohibit access by the PC to the corporate network until authentication with the authentication server passes AND an audit with the software agent with the GK passes, while still supporting the existing encryption and authentication functionality. The method used to support auditing functionality over the existing 802.1x protocol implementation is complicated and not an obvious variation of the 802.1x protocol.

In the invention, the auditing protocol takes place between the EP agent software and the GK. A client filter redirects calls for audit information to an agent on the EP and sends the responses to the 802.1x compliant AP which relays them to the EAP server. The EAP server then calls a server filter which sends the responses to the GK for evaluation. The GK sends requests for more information on the reverse path and this continues until the audit is completed. If the audit is successful, the server sends a message to the AP which enables the EP's port allowing access for the PC. If the audit fails, the port on the AP is left disabled.

According to an exemplary embodiment, client filters (CF) and server filters (SF) are added along with an agent and GK to perform audits, as highlighted in Figure 4. There may be one or more instances of the CF and SF, which correspond to the separate EAP Authentication Modules (EAPM) that are supported. Note that the agent and GK are logical components. The functionality of the agent and GK can be embedded into the CF and SF, respectively, or in the case of the GK, may reside on a separate server.

The provisional on page 13 also provides that, if the GK determines the EP has failed the audit, the port for the client EP or "access device" is left disabled or "set to a restricted VLAN where the EP has limited network access. In either case, the EP is isolated from the company network until it successfully passes an audit with the GK" through the "security policy requirements." This

US7523484	Constructive Reduction to Practice (US60/513,080)
	functionality is confirmed on page 14, which provides that “full or limited access to a corporate network can be provided based on the policy by setting the port to the VLAN” for the access device: <u>Pages 13-14</u> If the audit indicates the client EP is in compliance, the SF returns a success response. If the VLAN for the EP is specified in the policy, then the VLAN that should be used for this EP is passed back as well. If the GK determines that the EP has failed the audit, GK returns a failure response to SF which causes one of the following: (1) the SF returns a failure to ECL, and the corresponding port on the AP is left disabled, or (2) the SF returns a success response to the ECL but specifies that the EP should be set to a restricted VLAN where the EP has limited network access. In either case, the EP is isolated from the company network until it successfully passes an audit with the GK. 4. If the routers used by the protected VLANs support ACLs, full or limited access to the corporate network can be provided based on the policy by setting the port to the VLAN whose router interface has the desired ACL. As another example, the figure on page 21 provides that a security policy with requirements that must be satisfied before an access device is granted access to a less-restricted subset of a protected network, as the figure demonstrates that the device is “audit[ed]” and a “failed audit” results in the device having “restrict[ed] access” to the corporate network on the “Restricted LAN”:



US7523484	Constructive Reduction to Practice (US60/513,080)
[1.2] a policy auditor configured to audit the access device using the at least one security policy, in response to a request to access the less-restricted subset of the protected network, the request being sent from the access device to the gatekeeper via a communication device; and	The '080 provisional provides a policy auditor (GK/CGServer), configured to audit the access device using the at least one security policy, in response to a request to access the less-restricted subset of the protected network, the request being sent from the access device (e.g user's PC) to the gatekeeper via a communication device (e.g. access point (AP)/switch/wireless). For example, page 3 provides that "access to a corporate network" is "granted or denied to an end point", such as a PC, as "determined by [security] policies which specify the audit criteria and types of access." This access may include access to a less-restricted subset of the network, which is requested when an EP attempts to connect to the corporate network through an AP (i.e., a communication device).

Page 3

1

**GATEKEEPER INVENTION FOR CONTROLLING
ACCESS TO A CORPORATE NETWORK USING 802.1x**

The invention is directed to controlling access to a corporate network based on audit criteria for end points. The amount of access granted or denied to an end point is determined by policies which specify the audit criteria and types of access.

Definitions

GK – The software that acts as a gatekeeper by granting or denying access to the corporate network from end points after auditing the end point based on certain criteria.

PC – A notebook, desktop PC, PDA, or similar computing device.

ND –Network device such as a network printer, which is normally incapable of running an agent.

EP – End point which can be a PC or ND.

AP – A switch or wireless access point (WAP) which is used to connect EPs to the corporate network. An EP connects to a switch with an Ethernet cable to one of the switch's ports. An EP typically connects to a WAP through a wireless network card, commonly through protocols like 802.11a or 802.11b.

Page 8 also supports this element, discloses that the GK performs the audit in response to a request to access the less-restricted subset of the protected network, the request being sent from the access device

US7523484	Constructive Reduction to Practice (US60/513,080)
	(e.g., the EP) to the GK via a communication device (e.g., the AP). Page 8 further states “[i]f the audit is successful, the server sends a message to the AP which enables the EP’s port allowing access for the PC. . . .” which “allow[s] access to the less restricted subset of the network.” To access the corporate network, the device must pass an audit. (“an AP may be programmed to prohibit access... until an audit with the software agent with the GK passes...”).

Page 8

Invention

According to the invention, an AP may be programmed to prohibit access by the PC to the corporate network until authentication with the authentication server passes AND an audit with the software agent with the GK passes, while still supporting the existing encryption and authentication functionality. The method used to support auditing functionality over the existing 802.1x protocol implementation is complicated and not an obvious variation of the 802.1x protocol.

In the invention, the auditing protocol takes place between the EP agent software and the GK. A client filter redirects calls for audit information to an agent on the EP and sends the responses to the 802.1x compliant AP which relays them to the EAP server. The EAP server then calls a server filter which sends the responses to the GK for evaluation. The GK sends requests for more information on the reverse path and this continues until the audit is completed. If the audit is successful, the server sends a message to the AP which enables the EP's port allowing access for the PC. If the audit fails, the port on the AP is left disabled.

According to an exemplary embodiment, client filters (CF) and server filters (SF) are added along with an agent and GK to perform audits, as highlighted in Figure 4. There may be one or more instances of the CF and SF, which correspond to the separate EAP Authentication Modules (EAPM) that are supported. Note that the agent and GK are logical components. The functionality of the agent and GK can be embedded into the CF and SF, respectively, or in the case of the GK, may reside on a separate server.

The provisional on page 13 also provides that, if the GK determines the EP has failed the audit, the port for the client EP or "access device" is left disabled or "set to a restricted VLAN where the EP has limited network access. In either case, the EP is isolated from the company network until it successfully passes an audit with the GK" through the "security policy requirements." This

US7523484	Constructive Reduction to Practice (US60/513,080)
	functionality is confirmed on page 14, which provides that “full or limited access to a corporate network can be provided based on the policy by setting the port to the VLAN” for the access device: <u>Pages 13-14</u> If the audit indicates the client EP is in compliance, the SF returns a success response. If the VLAN for the EP is specified in the policy, then the VLAN that should be used for this EP is passed back as well. If the GK determines that the EP has failed the audit, GK returns a failure response to SF which causes one of the following: (1) the SF returns a failure to ECL, and the corresponding port on the AP is left disabled, or (2) the SF returns a success response to the ECL but specifies that the EP should be set to a restricted VLAN where the EP has limited network access. In either case, the EP is isolated from the company network until it successfully passes an audit with the GK. 4. If the routers used by the protected VLANs support ACLs, full or limited access to the corporate network can be provided based on the policy by setting the port to the VLAN whose router interface has the desired ACL. As another example, the figures on pages 19 and 21 provide that a security policy with requirements that must be satisfied before an access device is granted access to a less-restricted subset of a protected network, as the figure demonstrates that the device is “audit[ed]” and a “failed audit” results in the device having “restrict[ed] access” to the corporate network on the “Restricted LAN”. Notably, the figure on page 19 discloses that the first step is that the “PC attaches to switch (VLAN is restricted by default)” and that, on page 21, the first step is that the “[u]ser connects to network,” both of which

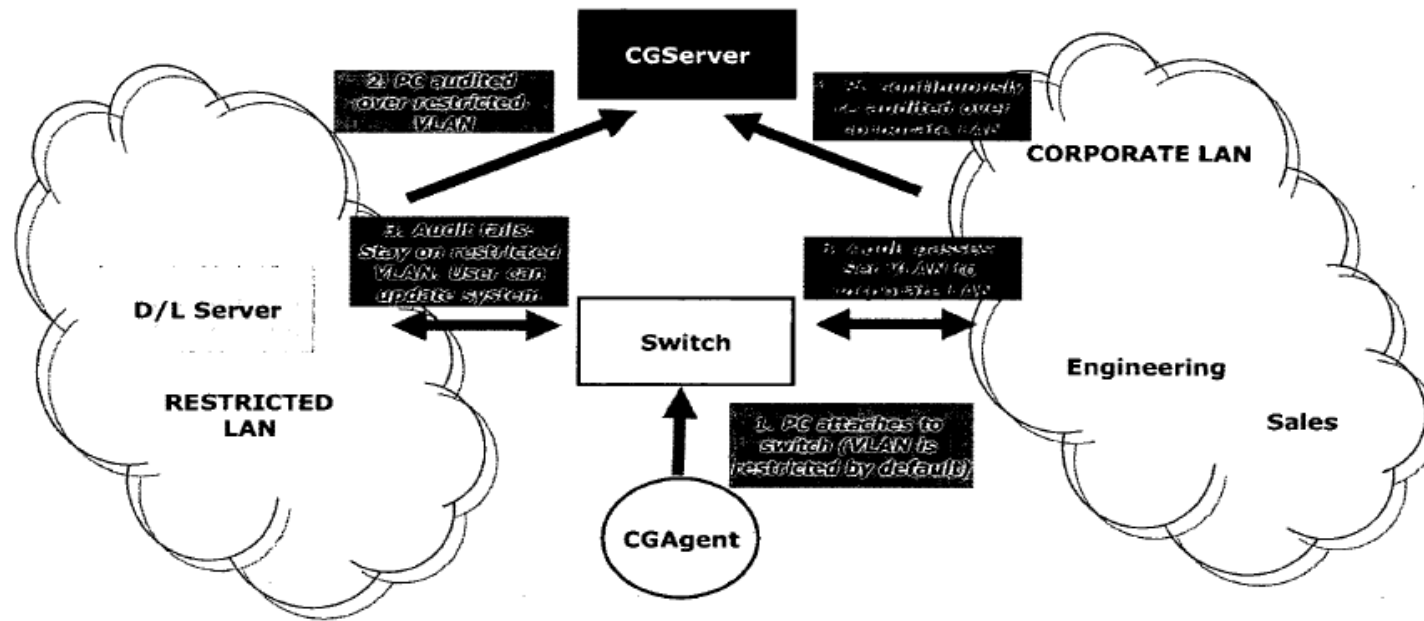
US7523484

Constructive Reduction to Practice (US60/513,080)

disclose that the user requests access to the less-restricted subset of the network and that the auditing is done in response to that request:

Page 19

LAN Mode
Normal traffic does not traverse CGS



(c) 2003 InfoExpress, Inc.

4

US7523484	Constructive Reduction to Practice (US60/513,080)
	Page 21 Audit Mode Client Side Enforcement The diagram illustrates the 'Audit Mode Client Side Enforcement' architecture. It features two main network environments: a RESTRICTED LAN on the left and a CORPORATE LAN on the right. The RESTRICTED LAN contains a D/L Server. The CORPORATE LAN includes Engineering and Sales departments. A central VPN/NAS/Switch connects these two LANs. Above the switch is a CG Server, and below it is a CGAgent. The process flow is indicated by numbered steps: 1. 'User connects to network' (arrow from Corporate LAN to Switch); 2. 'System audited and re-audited' (arrow from Switch to CG Server); 3. 'Failed audit: Agent restricts access' (arrow from CGAgent to Restricted LAN); and 4. 'Audit passes: Agent allows traffic' (arrow from CGAgent to Corporate LAN).
[1.3] an access control configured to reconfigure the communication device such that data sent from	See claim 1.1 and 1.2. The '080 provisional discloses an access control configured to reconfigure the communication device (e.g. network access point) such that data sent from the access device is received by the less-restricted subset of the protected network rather than merely a restricted subset of the protected network, if the audit results in a determination that the access device meets the requirements of the at least one security policy, the restricted subset of the protected network including the gatekeeper.

US7523484	Constructive Reduction to Practice (US60/513,080)
the access device is received by the less-restricted subset of the protected network rather than merely a restricted subset of the protected network, if the audit results in a determination that the access device meets the requirements of the at least one security policy, the restricted subset of the protected network including the gatekeeper.	For example, page 8 provides that “[i]f the audit is successful, the server sends a message to the AP which enables the EP’s port allowing access for the PC. . . .” This process of “send[ing] a message to an [access point]” shows “reconfiguring the communication port” thereupon. Additionally, because this reconfiguring “enables the EP’s port allowing access for the PC,” the reconfiguring permits “communicating data between the access device and the less-restricted subset of the protected network.” Finally, because this process happens “[i]f the audit is successful,” the reconfiguring takes place “when the requirements of the security policy are satisfied”.

US7523484	Constructive Reduction to Practice (US60/513,080)
	Invention According to the invention, an AP may be programmed to prohibit access by the PC to the corporate network until authentication with the authentication server passes AND an audit with the software agent with the GK passes, while still supporting the existing encryption and authentication functionality. The method used to support auditing functionality over the existing 802.1x protocol implementation is complicated and not an obvious variation of the 802.1x protocol. In the invention, the auditing protocol takes place between the EP agent software and the GK. A client filter redirects calls for audit information to an agent on the EP and sends the responses to the 802.1x compliant AP which relays them to the EAP server. The EAP server then calls a server filter which sends the responses to the GK for evaluation. The GK sends requests for more information on the reverse path and this continues until the audit is completed. If the audit is successful, the server sends a message to the AP which enables the EP's port allowing access for the PC. If the audit fails, the port on the AP is left disabled. According to an exemplary embodiment, client filters (CF) and server filters (SF) are added along with an agent and GK to perform audits, as highlighted in Figure 4. There may be one or more instances of the CF and SF, which correspond to the separate EAP Authentication Modules (EAPM) that are supported. Note that the agent and GK are logical components. The functionality of the agent and GK can be embedded into the CF and SF, respectively, or in the case of the GK, may reside on a separate server. As another example, pages 13-14 provide that the "EP is isolated from the company network until it successfully passes an audit with the GK." That is, access to the company network is restricted by default, and the AP must be reconfigured in order to grant access. Page 14 also provides that the GK may "control many different ports and APs [] from a different network," which a POSITA would

US7523484	Constructive Reduction to Practice (US60/513,080)
	understand to include the restricted subset of the protected network or “Restricted LAN”. Furthermore, page 14 and other portions of the specification describe the invention as not “requiring normal network traffic to traverse the [gatekeeper]”—and thus reconfiguring “the communication device such that data sent from the access device is received by the less-restricted subset of the protected network rather than merely a restricted subset of the protected network, if the audit results in a determination that the access device meets the requirements of the at least one security policy, the restricted subset of the protected network including the gatekeeper.” <u>Page 13</u> If the audit indicates the client EP is in compliance, the SF returns a success response. If the VLAN for the EP is specified in the policy, then the VLAN that should be used for this EP is passed back as well. If the GK determines that the EP has failed the audit, GK returns a failure response to SF which causes one of the following: (1) the SF returns a failure to ECL, and the corresponding port on the AP is left disabled, or (2) the SF returns a success response to the ECL but specifies that the EP should be set to a restricted VLAN where the EP has limited network access. In either case, the EP is isolated from the company network until it successfully passes an audit with the GK.

Page 14

2. An EP attached to a port on the AP can be restricted from accessing the corporate network if it does not meet audit criteria. There is no need to physically insert a GK between the EP and the AP
3. The invention is highly scalable because a single GK can control many different ports and APs (i) from a different network, (ii) without a direct connection to the AP, and (iii) without requiring normal network traffic to traverse the GK.
4. If the routers used by the protected VLANs support ACLs, full or limited access to the corporate network can be provided based on the policy by setting the port to the VLAN whose router interface has the desired ACL.
5. The invention adds the ability to audit EPs that support an API where the audit filters can be inserted, without the need to change the existing authentication and encryption methods.

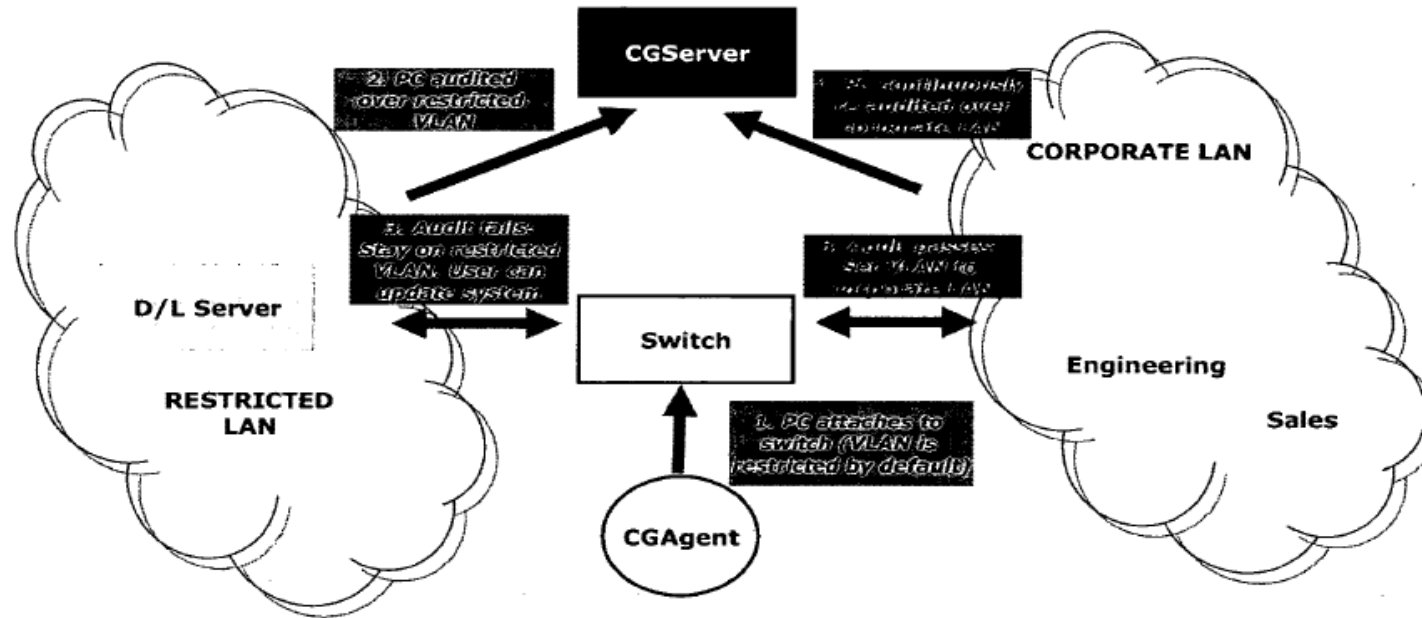
Details of exemplary enforcement modes of the invention are given in the attached Appendix.

This functionality is also provided by the figure on page 19, which demonstrates that, in the “LAN Mode,” the “[n]ormal traffic does not traverse the [server]”—that is the claimed gatekeeper. Instead, the endpoint (as shown by the CG Agent) can communicate directly with the corporate LAN without going through the CG server.

Page 19

LAN Mode

Normal traffic does not traverse CGS



(c) 2003 InfoExpress, Inc.

4

On page 21, the provisional depicts two alternate scenarios—one where the “audit passes” and the “agent allows access” to the corporate LAN (that is, the “less restricted subset of the network”), and another where the “audit fails” and the “agent restricts access” to the “restricted LAN.” It is apparent that this shows the “out of band” architecture described above.

US7523484	Constructive Reduction to Practice (US60/513,080)
	Page 21 Audit Mode Client Side Enforcement The diagram illustrates a network architecture for 'Audit Mode Client Side Enforcement'. At the top center is a box labeled 'CG Server'. Below it is a box labeled 'VPN/NAS/Switch'. To the left of the switch is a cloud labeled 'RESTRICTED LAN' containing a box labeled 'D/L Server'. To the right of the switch is a cloud labeled 'CORPORATE LAN' containing boxes labeled 'Engineering' and 'Sales'. At the bottom center is a circle labeled 'CGAgent'. Arrows indicate connections: a double-headed arrow between the 'RESTRICTED LAN' cloud and the 'VPN/NAS/Switch' box; a double-headed arrow between the 'CORPORATE LAN' cloud and the 'VPN/NAS/Switch' box; an arrow pointing from the 'VPN/NAS/Switch' box to the 'CG Server'; and an arrow pointing from the 'CGAgent' circle to the 'VPN/NAS/Switch' box. Four numbered steps are shown in boxes: '1. User connects to network' (between switch and corporate LAN), '2. System audited and re-audited' (between switch and CG server), '3. Failed audit Agent restricts access' (between switch and restricted LAN), and '4. Audit accesses Agent allows access' (between CGAgent and switch).
[2]	See [1.1]-[1.3]. The '080 provisional discloses a network gatekeeper is communicatively coupled with a router configured to limit access to only the restricted subset using an access control list.

US7523484	Constructive Reduction to Practice (US60/513,080)
	For example, pages 13-14 disclose that full or limited access to a the corporate network through a router coupled with a GK configured to limit access to only a restricted subset or “desired ACL” (access control list): <u>Page 13</u> If the GK determines that the EP has failed the audit, GK returns a failure response to SF which causes one of the following: (1) the SF returns a failure to ECL, and the corresponding port on the AP is left disabled, or (2) the SF returns a success response to the ECL but specifies that the EP should be set to a restricted VLAN where the EP has limited network access. In either case, the EP is isolated from the company network until it successfully passes an audit with the GK. After the audit has been performed, “keep alives” and updates regarding changes to previous audit information are exchanged. Changes are reevaluated and if inconsistent with the current state, access to the network is modified appropriately by changing the VLAN used for the EP or by terminating access by the EP by communicating with the AP. <u>Page 14</u> 4. If the routers used by the protected VLANs support ACLs, full or limited access to the corporate network can be provided based on the policy by setting the port to the VLAN whose router interface has the desired ACL. As provided on page 3, and a POSITA would understand, that the GK is communicatively coupled with a router as the ACL is applied to a router port or a switch port:

US7523484	Constructive Reduction to Practice (US60/513,080)
	<u>Page 3:</u> 1 GATEKEEPER INVENTION FOR CONTROLLING ACCESS TO A CORPORATE NETWORK USING 802.1x The invention is directed to controlling access to a corporate network based on audit criteria for end points. The amount of access granted or denied to an end point is determined by policies which specify the audit criteria and types of access. Definitions GK – The software that acts as a gatekeeper by granting or denying access to the corporate network from end points after auditing the end point based on certain criteria. PC – A notebook, desktop PC, PDA, or similar computing device. ND –Network device such as a network printer, which is normally incapable of running an agent. EP – End point which can be a PC or ND. AP – A switch or wireless access point (WAP) which is used to connect EPs to the corporate network. An EP connects to a switch with an Ethernet cable to one of the switch's ports. An EP typically connects to a WAP through a wireless network card, commonly through protocols like 802.11a or 802.11b. ACL – Access Control List, which is a set of filtering rules that specify what traffic is permitted through a port. In the following description, the ACL is the one applied to a router port or a switch port.

US7523484	Constructive Reduction to Practice (US60/513,080)
[3]	<i>See</i> [1]. The '080 provisional provides a network gatekeeper that is further configured to update the access device using an update module. Page 13 provides that if the EP fails the audit, the GK “returns a failure response” which is communicated back to the EP by denying access to the company network. A POSITA would understand that the gatekeeper may be configured to update the access device (GK is further configured to update the access device using an update module) because the GK communicates with and informs the device that the software is not up to date in response to a failed audit when the “GK returns a failure response.” <u>Page 13</u> If the GK determines that the EP has failed the audit, GK returns a failure response to SF which causes one of the following: (1) the SF returns a failure to ECL, and the corresponding port on the AP is left disabled, or (2) the SF returns a success response to the ECL but specifies that the EP should be set to a restricted VLAN where the EP has limited network access. In either case, the EP is isolated from the company network until it successfully passes an audit with the GK. After the audit has been performed, “keep alives” and updates regarding changes to previous audit information are exchanged. Changes are reevaluated and if inconsistent with the current state, access to the network is modified appropriately by changing the VLAN used for the EP or by terminating access by the EP by communicating with the AP.

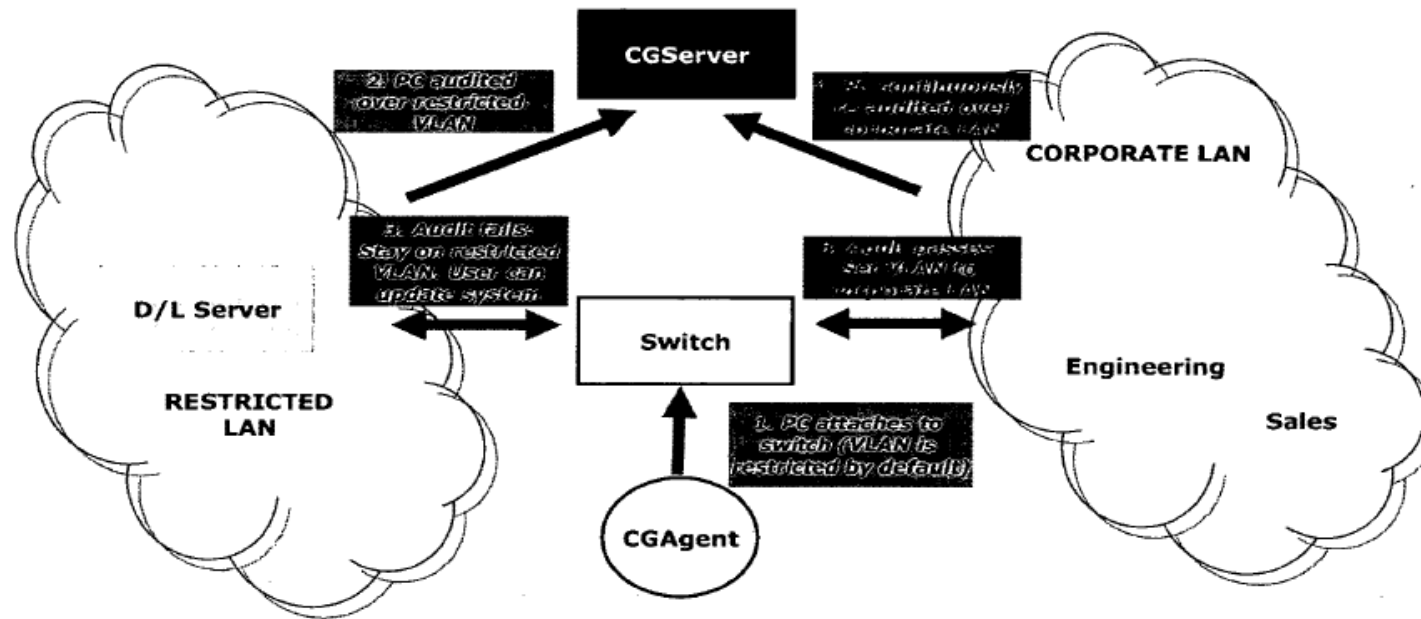
US7523484

Constructive Reduction to Practice (US60/513,080)

This is further demonstrated by the figures on pages 19 and 20, which provide that when an “audit fails...[u]ser can update system” and that after a “failed audit...[u]ser must update system,” which as demonstrated in the figure below a POSITA would understand could be accomplished through the GK or “CGServer”:

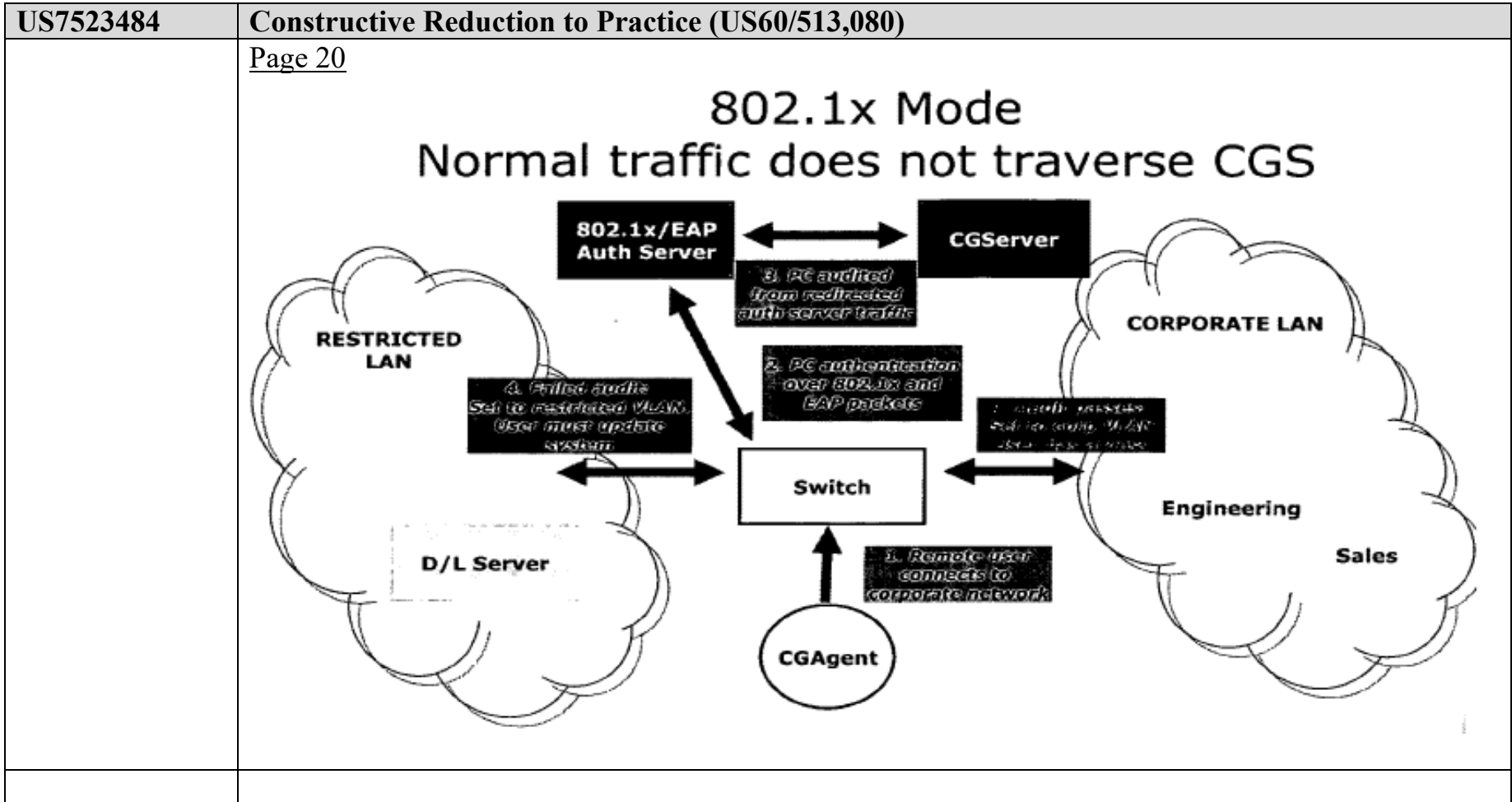
Page 19:

LAN Mode
Normal traffic does not traverse CGS



(c) 2003 InfoExpress, Inc.

4



US7523484	Constructive Reduction to Practice (US60/513,080)
[4]	<i>See [1].</i> The provisional provides that the network gatekeeper is configured to obtain system data from the access device. For example, on page 4, the provisional provides that the “agent tells the GK information about the EP including applications configurations, and user logins,” which is system data from the access device via the agent (e.g. CG Agent) running on the access device. <u>Page 4</u> When the EP tries to access the corporate network, a software agent running on the EP automatically conducts an audit session with the GK. The agent tells the GK information about the EP including applications, configurations, and user logins, which the GK compares against the policies from the policy manager. Page 8 also provides that the auditing protocol “takes place between the EP agent software and the GK,” where the GK “sends requests for more information” and obtains the information from the access device until the audit is completed:

Page 8

Invention

According to the invention, an AP may be programmed to prohibit access by the PC to the corporate network until authentication with the authentication server passes AND an audit with the software agent with the GK passes, while still supporting the existing encryption and authentication functionality. The method used to support auditing functionality over the existing 802.1x protocol implementation is complicated and not an obvious variation of the 802.1x protocol.

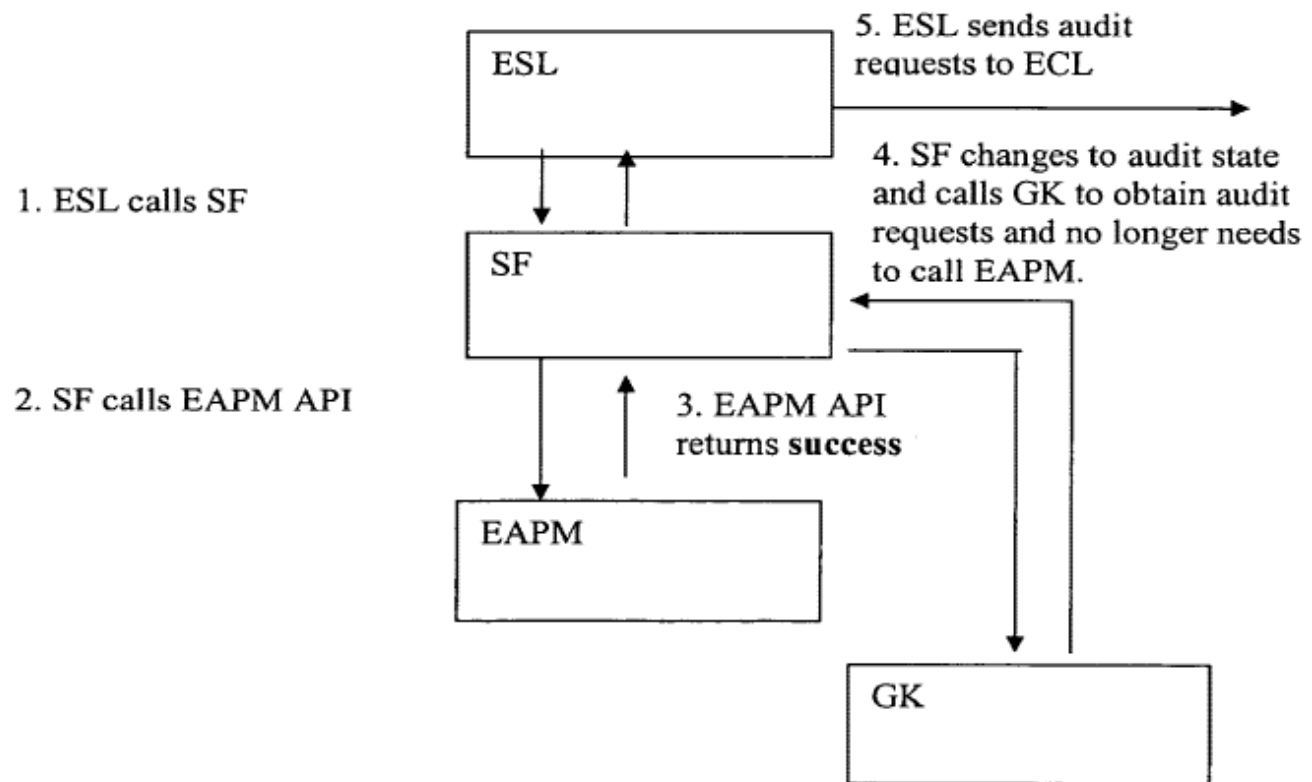
In the invention, the auditing protocol takes place between the EP agent software and the GK. A client filter redirects calls for audit information to an agent on the EP and sends the responses to the 802.1x compliant AP which relays them to the EAP server. The EAP server then calls a server filter which sends the responses to the GK for evaluation. The GK sends requests for more information on the reverse path and this continues until the audit is completed. If the audit is successful, the server sends a message to the AP which enables the EP's port allowing access for the PC. If the audit fails, the port on the AP is left disabled.

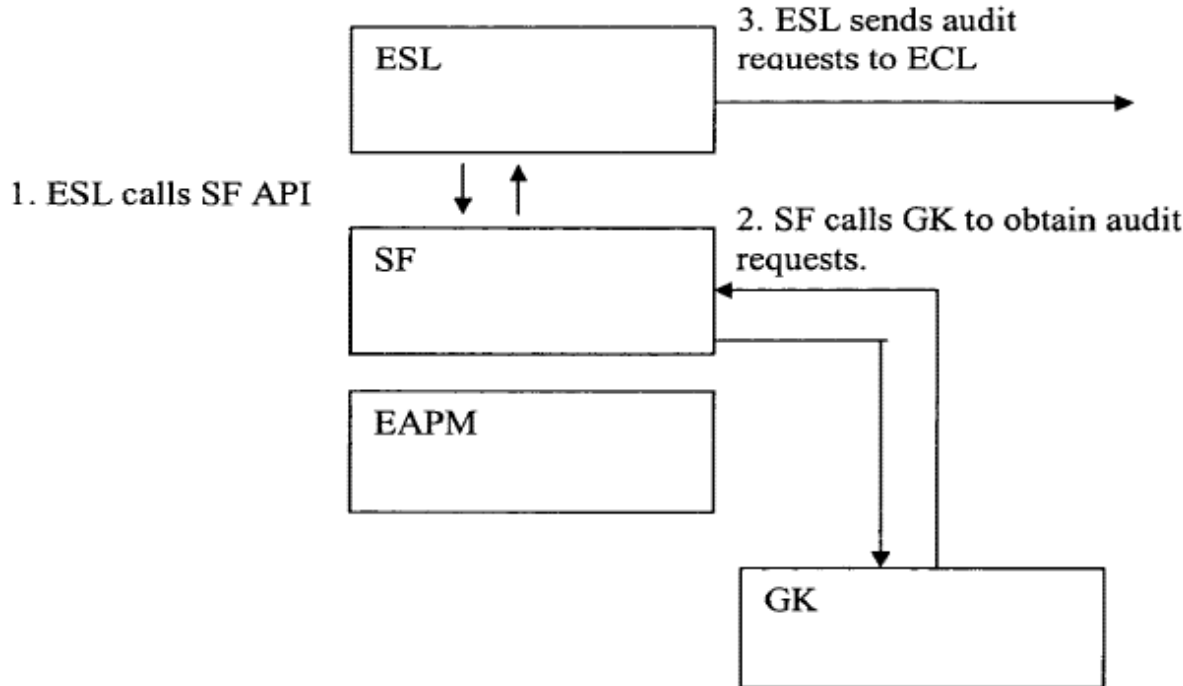
Pages 11-12 and figures 6 and 7a also provide that the audit requests from the "agent API" are obtained by the "GK":

Page 11

On the client, audit requests are passed to the agent API instead of to the client EAPM. The agent returns information about the local system, which is converted to audit responses that are sent to the server.

Figure 6: Server Changing to Audit State



US7523484	Constructive Reduction to Practice (US60/513,080)
	<u>Page 12</u> During the audit state, the SF and CF exchange audit requests and responses about the EP as shown in Figures 7a and 7b. The ECL and ESL continue to communicate with the CF and SF, but instead of calling the EAPM, the CF and SF call the agent and GK respectively, to perform this exchange. The audit session continues until the necessary audit information has been passed to the SF. Figure 7a: Server in Audit State  <pre> sequenceDiagram participant ESL participant SF participant EAPM participant GK ESL->>SF: 1. ESL calls SF API SF->>GK: 2. SF calls GK to obtain audit requests. ESL->>ECL: 3. ESL sends audit requests to ECL </pre> The diagram illustrates the sequence of operations during an audit state. It features four main components: ESL (top), SF (middle), EAPM (bottom left), and GK (bottom right). The process begins with ESL calling the SF API, indicated by a downward arrow labeled '1. ESL calls SF API'. This is followed by SF calling GK to obtain audit requests, shown by a downward arrow from SF to GK labeled '2. SF calls GK to obtain audit requests.'. A third step, '3. ESL sends audit requests to ECL', is shown as an arrow pointing right from ESL. Additionally, there is a bidirectional vertical arrow between ESL and SF, suggesting ongoing communication between them.

US7523484	Constructive Reduction to Practice (US60/513,080)
[5]	<i>See</i> [1] and [4]. The provisional supports the limitation of the network gatekeeper further configured to use the system data to determine if the access device meets requirements of a security policy, and to issue commands responsive to this determination, the commands being configured to grant access to the less-restricted subset. For example, Page 8 describes how an endpoint is “isolated from the company network until it successfully passes an audit.” That is, access to the company network is restricted by default, and commands must be issued in response to a successful audit in order to grant access.

Page 8

If the audit indicates the client EP is in compliance, the SF returns a success response. If the VLAN for the EP is specified in the policy, then the VLAN that should be used for this EP is passed back as well.

If the GK determines that the EP has failed the audit, GK returns a failure response to SF which causes one of the following: (1) the SF returns a failure to ECL, and the corresponding port on the AP is left disabled, or (2) the SF returns a success response to the ECL but specifies that the EP should be set to a restricted VLAN where the EP has limited network access. In either case, the EP is isolated from the company network until it successfully passes an audit with the GK.

After the audit has been performed, “keep alives” and updates regarding changes to previous audit information are exchanged. Changes are reevaluated and if inconsistent with the current state, access to the network is modified appropriately by changing the VLAN used for the EP or by terminating access by the EP by communicating with the AP.

Page 14 also describes the network GK granting “full or limited access to the corporate network . . . based on the policy” based on whether the access device meets the requirements of the auditing protocol or security policy. It does so by issuing commands, i.e., “control[ing] many different ports and APs.”

Page 14

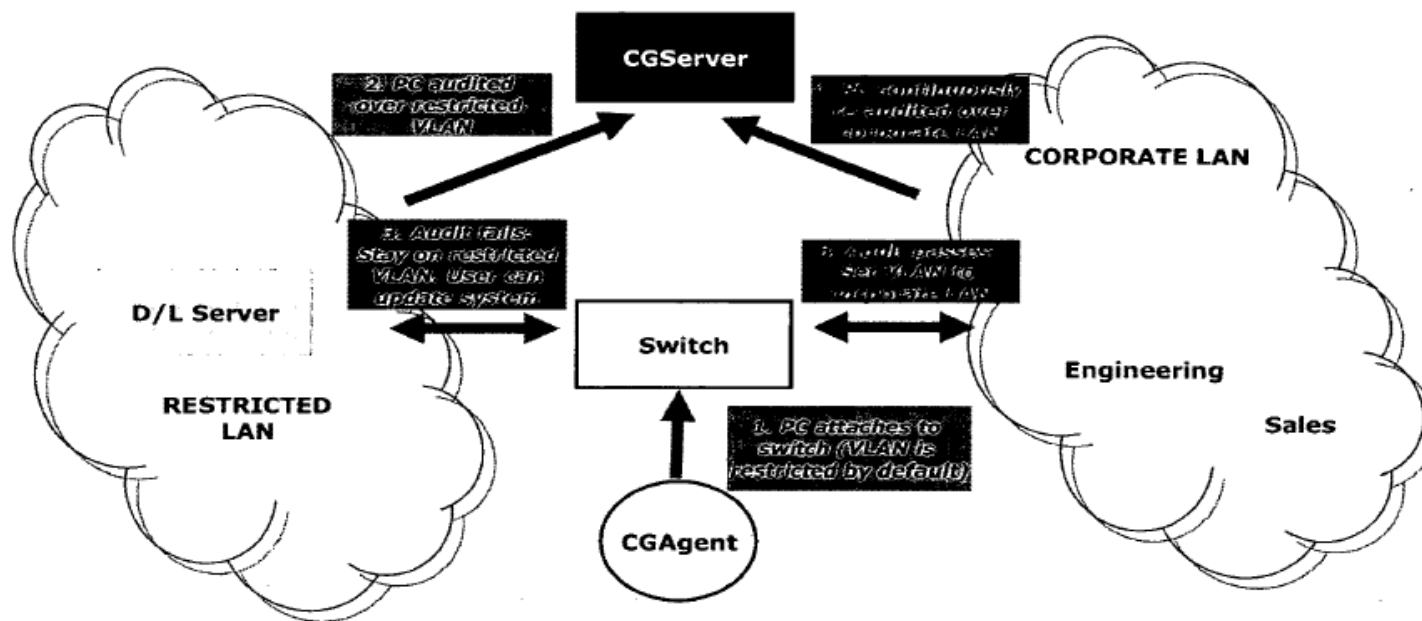
2. An EP attached to a port on the AP can be restricted from accessing the corporate network if it does not meet audit criteria. There is no need to physically insert a GK between the EP and the AP
3. The invention is highly scalable because a single GK can control many different ports and APs (i) from a different network, (ii) without a direct connection to the AP, and (iii) without requiring normal network traffic to traverse the GK.
4. If the routers used by the protected VLANs support ACLs, full or limited access to the corporate network can be provided based on the policy by setting the port to the VLAN whose router interface has the desired ACL.
5. The invention adds the ability to audit EPs that support an API where the audit filters can be inserted, without the need to change the existing authentication and encryption methods.

As provided in the figures on pages 19 and 20, upon determining that the “audit passes” the user device may be sent to the Corporate LAN (i.e., the less-restricted subset) by the GK.

Page 19

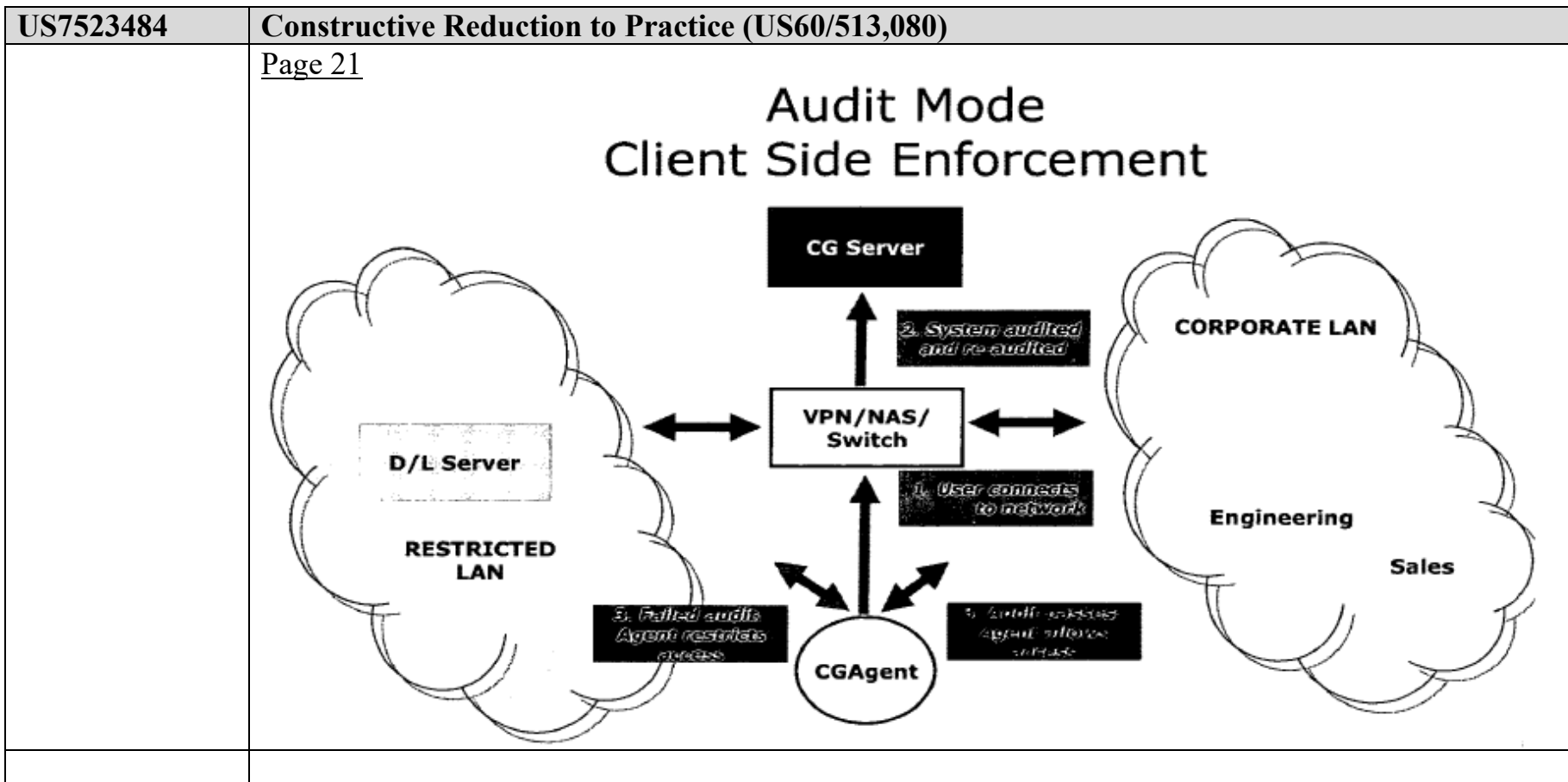
LAN Mode

Normal traffic does not traverse CGS



(c) 2003 InfoExpress, Inc.

4

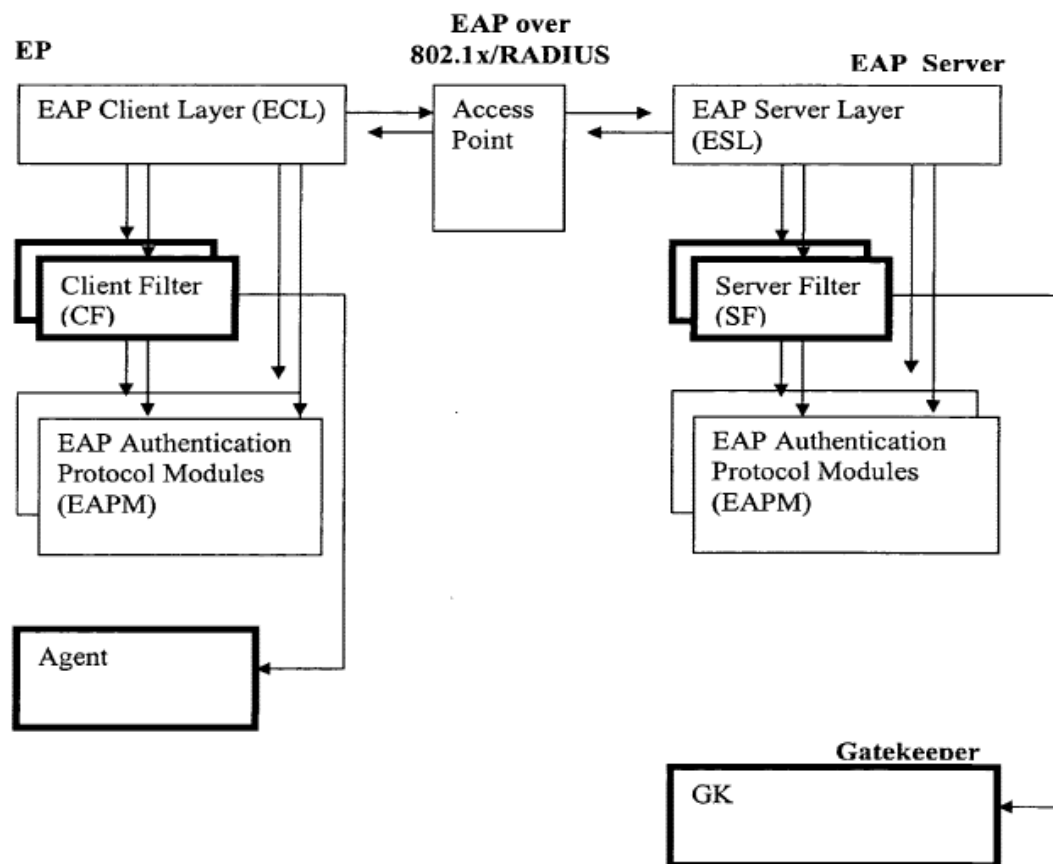


US7523484	Constructive Reduction to Practice (US60/513,080)
[6]	<i>See</i> [1] and [4]. Page 11 states, “On the client, audit requests are passed to the agent API instead of to the client EAPM. The agent returns information about the local system, which is converted to audit responses that are sent to the server.” A POSITA would understand that the “information about the local system” supports wherein the system data includes antivirus software version data. <u>Page 11</u> The ECL calls the corresponding CF to perform authentication, which at first calls the appropriate EAPM to obtain the proper authentication response. The authentication response is returned by the CF to the ESL, which sends the response to the server’s ESL, SF, and EAPM. This process continues until the authentication either succeeds or fails, at which time the server’s authentication EAPM returns a success or failure response to the SF. If the SF receives a success response from the server EAPM as shown in Figure 6, the SF changes to the audit state and calls GK to obtain audit requests to send back to the client. In this state, the SF returns specially formatted audit requests to the ESL which are passed to the ECL, and eventually to the CF which sends back audit responses to the SF requests. On the client, audit requests are passed to the agent API instead of to the client EAPM. The agent returns information about the local system, which is converted to audit responses that are sent to the server. Additionally, the references to the types of device information that were absent from prior art access control systems—e.g. that regarding a “virus or trojan running on [the endpoints]” (pages 5-6)—mean that a POSITA would understand that in the present invention “the system data includes antivirus software version data.”

US7523484	Constructive Reduction to Practice (US60/513,080)
[11]	<i>See</i> [1] and [6]. As explained above with respect to claim 6, the provisional supports [t]he network gatekeeper of claim 1, wherein the at least one security policy is responsive to an identity of the access device. The provisional discusses collecting “information about the local system”. A POSITA would understand that this information can include information about the identity of the device. The provisional, when discussing 802.1x which is used by the system described by the provisional, discusses that authentication relies on “authentication credentials, such as user name and password or a digital certificate.” And that “[a]lternatively, the PC can send some or all of the authentication credentials automatically without user intervention.” (Page 6.) A POSITA would also understand the client-side digital certificates are typically device dependent. A unique client-side digital certificate is created and put on the client device and the provisional supports using this for authentication (i.e., “at least one security policy”). A POSITA would understand that this digital certificate, which can be sent without user intervention, may be used for user authentication and/or device authentication. Therefore, a POSITA would understand that the present invention supported wherein at least one security policy is responsive to an identity of the access device. The diagrams in Figures 4, 5a & 5b, and in appendix page 20 depict the exchange of authentication information using 802.1x, including “information concerning an identity of a user of the device.”. This authentication information may include the digital certificate.

Page 9

Figure 4



Page 10

8

Figure 5a: Client in Authentication State

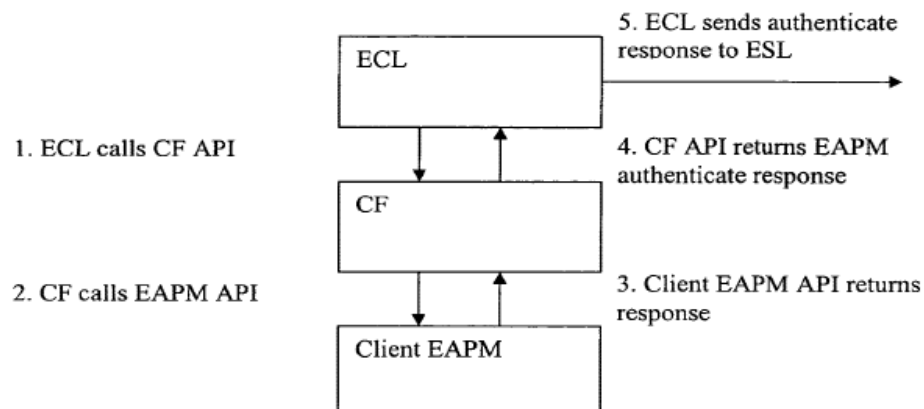
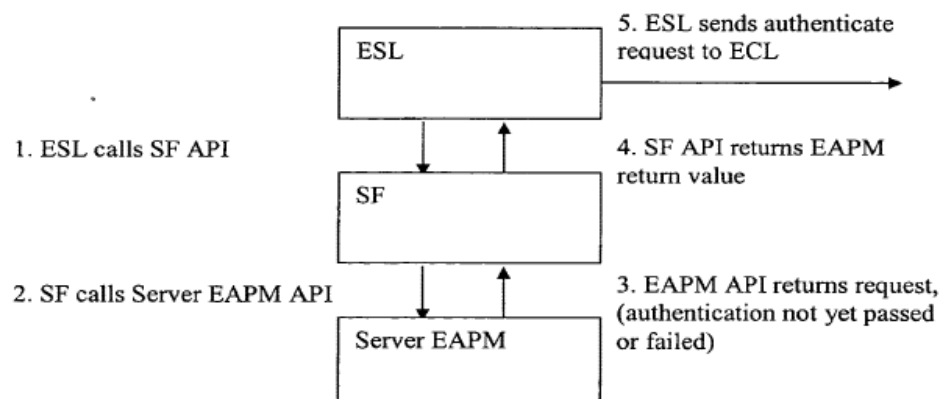


Figure 5b: Server in Authentication State



US7523484	Constructive Reduction to Practice (US60/513,080)
	Page 20 The diagram illustrates the 802.1x Mode network architecture. At the top, a banner reads "infoExpress Secure the last mile". Below this, the title "802.1x Mode" is followed by the statement "Normal traffic does not traverse CGS". The network consists of a central "Switch" connected to three main components: a "RESTRICTED LAN" on the left, a "CORPORATE LAN" on the right, and a "CGAgent" at the bottom. The "RESTRICTED LAN" contains a "D/L Server". The "CORPORATE LAN" contains "Engineering" and "Sales" departments. Above the switch are two servers: "802.1x/EAP Auth Server" and "CGServer", which are connected to each other and to the switch. The diagram shows four numbered steps in the authentication process: 1. "Remote user connects to corporate network" (CGAgent to Switch); 2. "PC authentication over 802.1x and EAP packets" (Switch to CGServer); 3. "PC audited from redirected auth server traffic" (CGServer to 802.1x/EAP Auth Server); 4. "Failed audit Set to restricted VLAN. User must update system" (802.1x/EAP Auth Server to Switch). A note at the bottom right of the diagram area says "5". (c) 2003 InfoExpress, Inc.

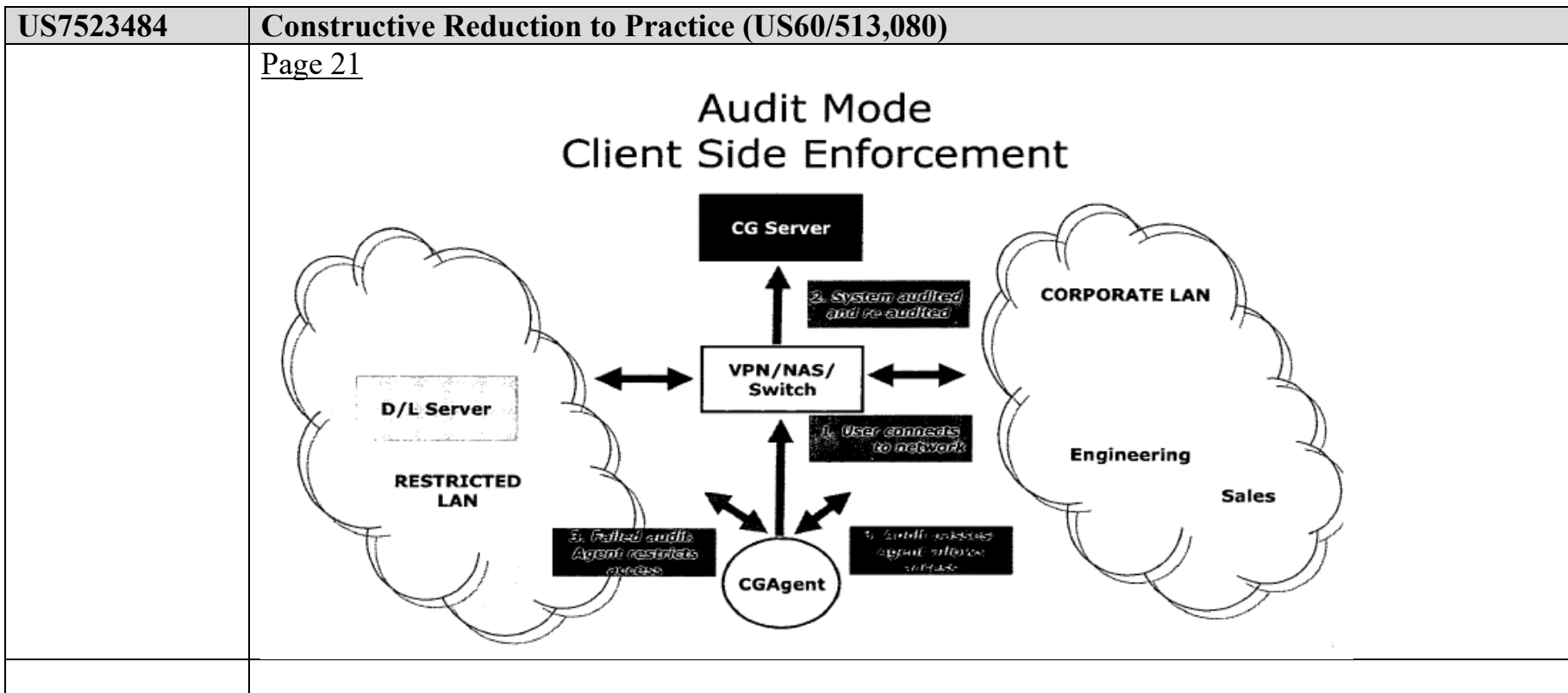
US7523484	Constructive Reduction to Practice (US60/513,080)
[12]	<i>See</i> [1], including claims [1.2] (for the “at least one security policy” limitation) and [1.3]. Page 11 and figure 6 provide that the SF in the “audit state” “calls the GK to obtain audit requests to send back to the client,” thereby providing the one security policy selected by the policy auditor. For example, a POSITA would understand that if the user device was seeking access on a protected network where there was only one less-restricted subset of the protected network, the request would have to be for access to the one “less-restricted subset” and the security policy would be specific to that “less-restricted subset”. The provisional states full or limited access to the corporate network can be provided (<i>see</i> page 14 below). A POSITA would understand that giving full or limited access to the corporate network would be based on the access that is requested (e.g. access device is only allowed access to part of the corporate network, the request to connect to the network would be limited to that portion of the network”). <u>Pages 14</u> 4. If the routers used by the protected VLANs support ACLs, full or limited access to the corporate network can be provided based on the policy by setting the port to the VLAN whose router interface has the desired ACL.

Page 11

The ECL calls the corresponding CF to perform authentication, which at first calls the appropriate EAPM to obtain the proper authentication response. The authentication response is returned by the CF to the ESL, which sends the response to the server's ESL, SF, and EAPM. This process continues until the authentication either succeeds or fails, at which time the server's authentication EAPM returns a success or failure response to the SF.

If the SF receives a success response from the server EAPM as shown in Figure 6, the SF changes to the audit state and calls GK to obtain audit requests to send back to the client. In this state, the SF returns specially formatted audit requests to the ESL which are passed to the ECL, and eventually to the CF which sends back audit responses to the SF requests.

On the client, audit requests are passed to the agent API instead of to the client EAPM. The agent returns information about the local system, which is converted to audit responses that are sent to the server.



US7523484	Constructive Reduction to Practice (US60/513,080)
[13]	<i>See</i> [1], [4], and [6]. For the same reasons as set forth in claim 6, the limitation of an audit responsive to antivirus software executing on the access device is disclosed. Page 11 states, “On the client, audit requests are passed to the agent API instead of to the client EAPM. The agent returns information about the local system, which is converted to audit responses that are sent to the server.” A POSITA would understand that the “information about the local system” supports “antivirus software executing on the access device.” <u>Page 11</u> The ECL calls the corresponding CF to perform authentication, which at first calls the appropriate EAPM to obtain the proper authentication response. The authentication response is returned by the CF to the ESL, which sends the response to the server’s ESL, SF, and EAPM. This process continues until the authentication either succeeds or fails, at which time the server’s authentication EAPM returns a success or failure response to the SF. If the SF receives a success response from the server EAPM as shown in Figure 6, the SF changes to the audit state and calls GK to obtain audit requests to send back to the client. In this state, the SF returns specially formatted audit requests to the ESL which are passed to the ECL, and eventually to the CF which sends back audit responses to the SF requests. On the client, audit requests are passed to the agent API instead of to the client EAPM. The agent returns information about the local system, which is converted to audit responses that are sent to the server.

US7523484	Constructive Reduction to Practice (US60/513,080)
	Additionally, the references to the types of device information that were absent, and therefore a problem with prior art access control systems included not verifying that a “virus or trojan running on [the endpoints]” (pages 5-6). A POSITA considering this problem in the provisional application would understand that in the present invention audit data includes information about “antivirus software executing on the access device.” <u>Page 6</u> A problem with this system is that it does not check whether or not the applications and configuration on the EP comply with corporate security policies. This means that users whose EPs have security vulnerabilities or EPs that have been breached (i.e., may have a virus or trojan running on them) can access the corporate network.
[15]	<i>See [1].</i> Page 12 and Figure 7a provide that the policy auditor is configured to request data from an agent on the access device, as the “SF and CF exchange audit requests and responses about the EP” and the “CF and SF call the agent and GK, respectively, to perform this exchange”:

US7523484	Constructive Reduction to Practice (US60/513,080)
	During the audit state, the SF and CF exchange audit requests and responses about the EP as shown in Figures 7a and 7b. The ECL and ESL continue to communicate with the CF and SF, but instead of calling the EAPM, the CF and SF call the agent and GK respectively, to perform this exchange. The audit session continues until the necessary audit information has been passed to the SF. Figure 7a: Server in Audit State <pre> sequenceDiagram participant ESL participant SF participant EAPM participant GK Note left of ESL: 1. ESL calls SF API ESL->>SF: SF->>ESL: Note left of SF: 2. SF calls GK to obtain audit requests. SF->>GK: Note right of ESL: 3. ESL sends audit requests to ECL ESL->>ECL: </pre> The diagram illustrates the sequence of operations during the audit state. It features four main components: ESL (top), SF (middle), EAPM (bottom left), and GK (bottom right). The process begins with ESL calling the SF API, indicated by a downward arrow from ESL to SF and an upward arrow from SF to ESL. Next, SF calls GK to obtain audit requests, shown by a downward arrow from SF to GK. Finally, ESL sends audit requests to ECL, represented by a horizontal arrow pointing right from ESL. The EAPM component is shown but has no active connections in this specific sequence.

US7523484	Constructive Reduction to Practice (US60/513,080)
[16]	<i>See</i> [1]. Page 3 provides that the communication device on the network gatekeeper includes a wireless access point (WAP):

US7523484	Constructive Reduction to Practice (US60/513,080)
	<u>Page 3</u> 1 GATEKEEPER INVENTION FOR CONTROLLING ACCESS TO A CORPORATE NETWORK USING 802.1x The invention is directed to controlling access to a corporate network based on audit criteria for end points. The amount of access granted or denied to an end point is determined by policies which specify the audit criteria and types of access. Definitions GK – The software that acts as a gatekeeper by granting or denying access to the corporate network from end points after auditing the end point based on certain criteria. PC – A notebook, desktop PC, PDA, or similar computing device. ND –Network device such as a network printer, which is normally incapable of running an agent. EP – End point which can be a PC or ND. AP – A switch or wireless access point (WAP) which is used to connect EPs to the corporate network. An EP connects to a switch with an Ethernet cable to one of the switch’s ports. An EP typically connects to a WAP through a wireless network card, commonly through protocols like 802.11a or 802.11b.

US7523484	Constructive Reduction to Practice (US60/513,080)
[17]	<i>See</i> [1] and [16]. The provisional provides that the WAP may be configured to support an 802.1x standard:

Page 3

1

**GATEKEEPER INVENTION FOR CONTROLLING
ACCESS TO A CORPORATE NETWORK USING 802.1x**

The invention is directed to controlling access to a corporate network based on audit criteria for end points. The amount of access granted or denied to an end point is determined by policies which specify the audit criteria and types of access.

Definitions

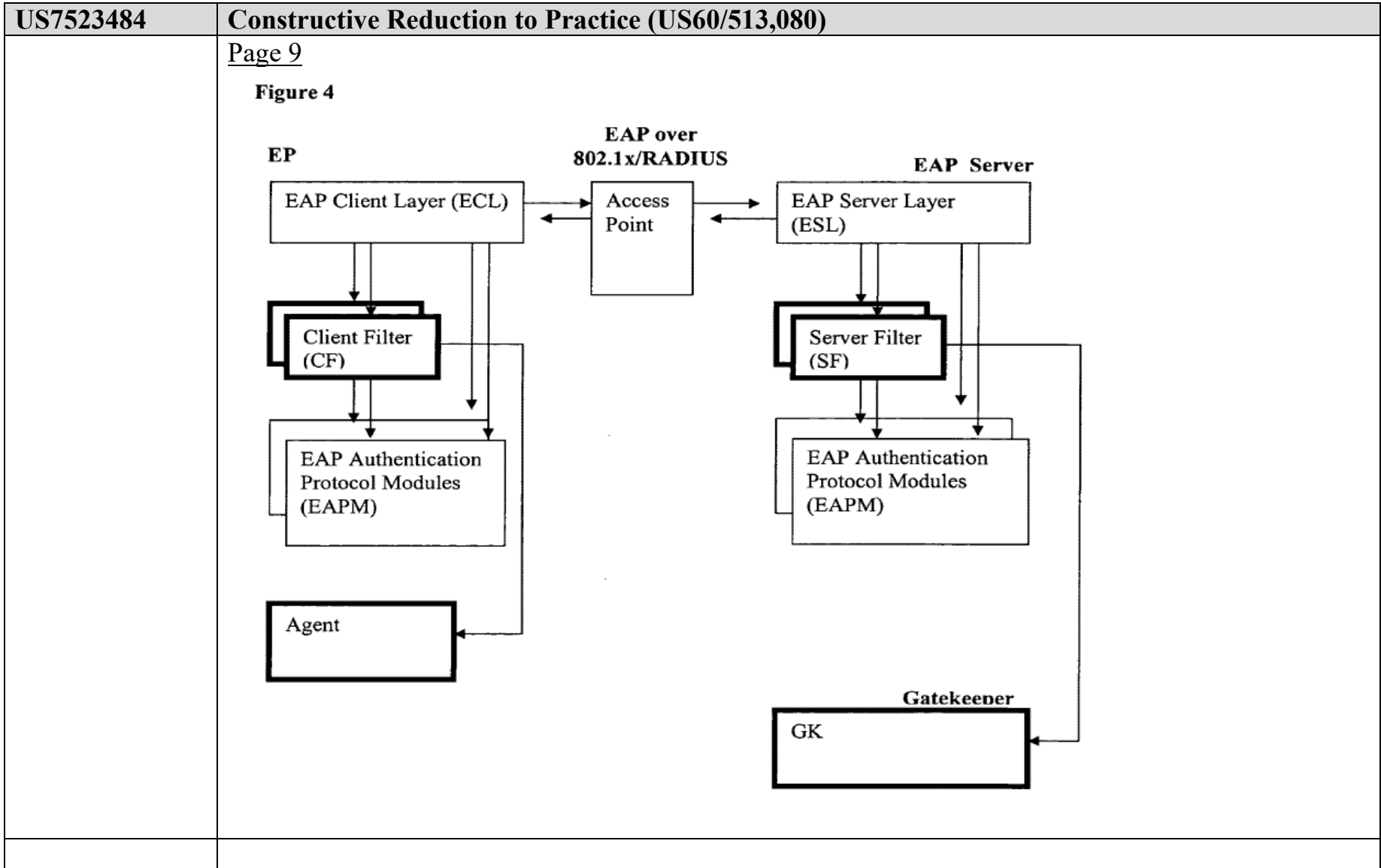
GK – The software that acts as a gatekeeper by granting or denying access to the corporate network from end points after auditing the end point based on certain criteria.

PC – A notebook, desktop PC, PDA, or similar computing device.

ND –Network device such as a network printer, which is normally incapable of running an agent.

EP – End point which can be a PC or ND.

AP – A switch or wireless access point (WAP) which is used to connect EPs to the corporate network. An EP connects to a switch with an Ethernet cable to one of the switch's ports. An EP typically connects to a WAP through a wireless network card, commonly through protocols like 802.11a or 802.11b.



US7523484	Constructive Reduction to Practice (US60/513,080)
[18]	<i>See</i> [1]. Page 3 provides that the communication device includes a network switch, of “[a] switch . . . which is used to connect to the EPs to the corporate network.”

Page 3

1

**GATEKEEPER INVENTION FOR CONTROLLING
ACCESS TO A CORPORATE NETWORK USING 802.1x**

The invention is directed to controlling access to a corporate network based on audit criteria for end points. The amount of access granted or denied to an end point is determined by policies which specify the audit criteria and types of access.

Definitions

GK – The software that acts as a gatekeeper by granting or denying access to the corporate network from end points after auditing the end point based on certain criteria.

PC – A notebook, desktop PC, PDA, or similar computing device.

ND –Network device such as a network printer, which is normally incapable of running an agent.

EP – End point which can be a PC or ND.

AP – A switch or wireless access point (WAP) which is used to connect EPs to the corporate network. An EP connects to a switch with an Ethernet cable to one of the switch's ports. An EP typically connects to a WAP through a wireless network card, commonly through protocols like 802.11a or 802.11b.

US7523484	Constructive Reduction to Practice (US60/513,080)
	Page 20 802.1x Mode Normal traffic does not traverse CGS (c) 2003 InfoExpress, Inc. 5

US7523484	Constructive Reduction to Practice (US60/513,080)
[19]	<i>See</i> [1] and [2]. The provisional discloses a network gatekeeper where the communication device includes a router. For example, page 3 provides that the invention includes an access control list (ACL) that is applied to a “router port”: <u>Page 3</u> ACL – Access Control List, which is a set of filtering rules that specify what traffic is permitted through a port. In the following description, the ACL is the one applied to a router port or a switch port. Page 14 also discloses “routers” may be “used by the protected VLANs support ACLs” to provide “full or limited access to the corporate network”. <u>Page 14</u> 4. If the routers used by the protected VLANs support ACLs, full or limited access to the corporate network can be provided based on the policy by setting the port to the VLAN whose router interface has the desired ACL.
[23]	<i>See</i> [1], [6], and [11]. As explained above with respect to claim 6, the provisional supports “[t]he network gatekeeper of claim 1, wherein the network gatekeeper is further configured to authenticate a user of the access device.” The provisional recognizes that authentication relies on “authentication credentials, such as user name and password or a digital certificate.” Page 6. In light this, a POSITA would understand that in the present invention, “the network gatekeeper is further configured to authenticate a user of the

US7523484	Constructive Reduction to Practice (US60/513,080)
	access device.” The diagrams in Figures 4, 5a & 5b, and in appendix page 20 depict the exchange of authentication information, including “authenticate a user of the access device.” <u>Page 9</u> Figure 4 <pre> graph TD subgraph EP ECL[EAP Client Layer (ECL)] CF[Client Filter (CF)] EAPM_EP[EAP Authentication Protocol Modules (EAPM)] Agent[Agent] ECL --> CF ECL --> EAPM_EP CF --> EAPM_EP EAPM_EP --> Agent end subgraph AP AP[Access Point] end subgraph EAP_Server ESL[EAP Server Layer (ESL)] SF[Server Filter (SF)] EAPM_ES[EAP Authentication Protocol Modules (EAPM)] GK[Gatekeeper (GK)] ESL --> SF ESL --> EAPM_ES SF --> EAPM_ES EAPM_ES --> GK end ECL <--> AP AP <--> ESL </pre>

Page 10

8

Figure 5a: Client in Authentication State

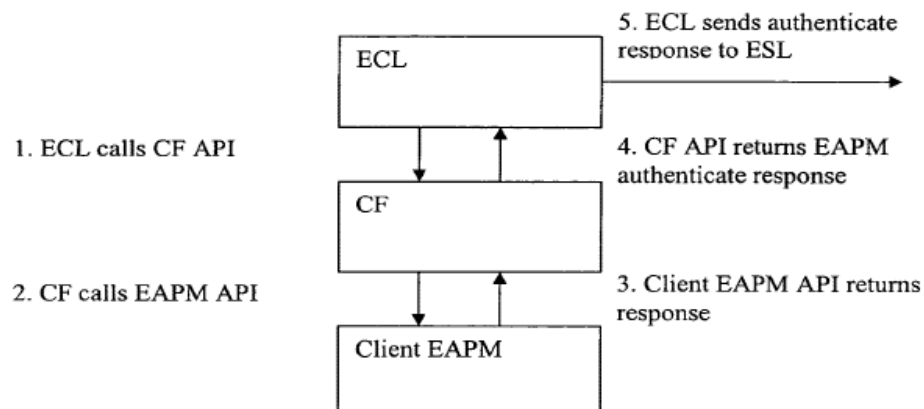
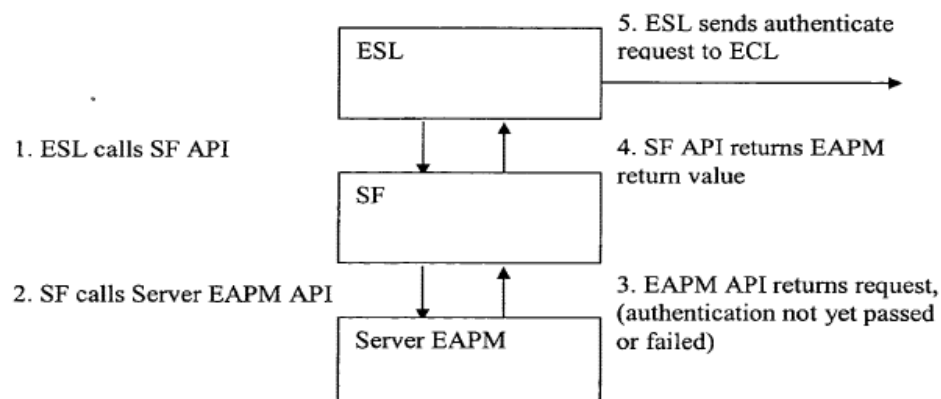
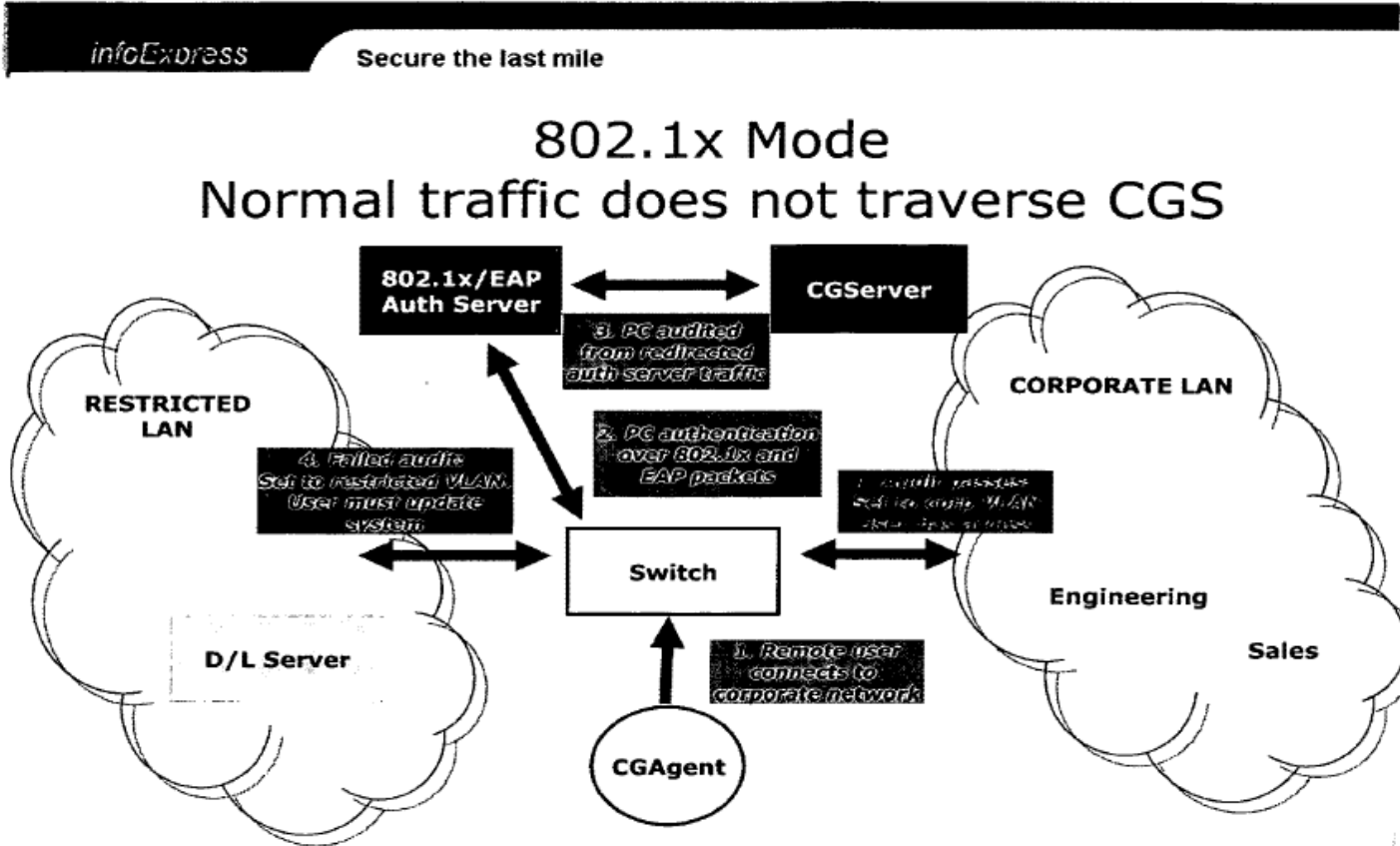


Figure 5b: Server in Authentication State

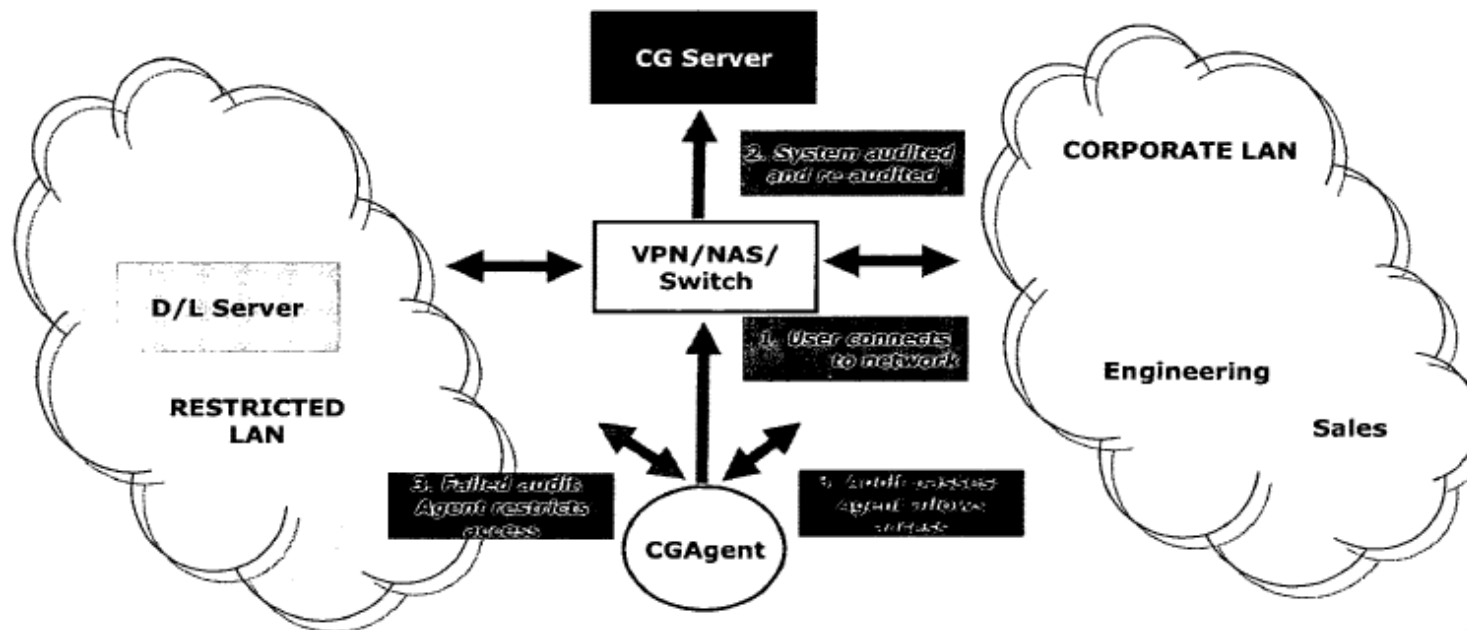


US7523484	Constructive Reduction to Practice (US60/513,080)
	Page 20  The diagram illustrates the 802.1x Mode network architecture. At the top, a banner reads "infoExpress Secure the last mile". Below this, the title "802.1x Mode" is followed by the statement "Normal traffic does not traverse CGS". The network consists of a central "Switch" connected to three main components: a "CGAgent" (represented by a circle), a "802.1x/EAP Auth Server", and a "CGServer" (represented by a rectangle). The "Switch" is also connected to two LANs: a "RESTRICTED LAN" on the left and a "CORPORATE LAN" on the right. The "RESTRICTED LAN" contains a "D/L Server". The "CORPORATE LAN" contains "Engineering" and "Sales" departments. The diagram shows the following steps in the authentication process: 1. Remote user connects to corporate network (indicated by an arrow from the Corporate LAN to the Switch). 2. PC authentication over 802.1x and EAP packets (indicated by a double-headed arrow between the Switch and the 802.1x/EAP Auth Server). 3. PC audited from redirected auth server traffic (indicated by a double-headed arrow between the 802.1x/EAP Auth Server and the CGServer). 4. Failed audit. Set to restricted VLAN. User must update system (indicated by a double-headed arrow between the Switch and the RESTRICTED LAN). At the bottom of the diagram, the text "(c) 2003 InfoExpress, Inc." and the page number "5" are visible.
[24]	See [1] and [3].

US7523484	Constructive Reduction to Practice (US60/513,080)
[25]	<i>See</i> [1]. The provisional describes using a communication device that includes a remote access virtual private network (VPN). The figure on page 21 demonstrates the communication device includes remote access using a VPN. The provisional also supports this limitation on page 3 and Figure 1, which describe that remote access using VPNs was well known at the time of the invention.

Page 21

Audit Mode Client Side Enforcement



US7523484	Constructive Reduction to Practice (US60/513,080)
	<u>Page 4</u> In a typical system, policies are created by a policy manager, which may be connected to the corporate network. The policies are transferred to a GK that sits between the network access server (NAS) used by the EP and the corporate network. This implies that the GK has two NICs, one for the NAS side and one for the corporate network side. Each policy indicates various combinations of applications, configurations, and user identity that are permitted or prohibited for an EP accessing the corporate network. The NAS may be a remote access VPN, dialup server, or any other type of remote access device which is provided to permit EPs to access the corporate network. See Figure 1.