ATTORNEY DOCKET NO. 09142.0002U1

16569 U.S. PTO
10/21/03

1

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

22387 U.S. PTO
60/513080
102103

This is a request for filing a **PROVISIONAL APPLICATION FOR PATENT** under 37 C.F.R. § 1.53(c).

	Docket Number	09142.0002U1	Type a Plus Sign (+) inside this box → → →	+

INVENTOR(s)/APPLICANT(s)

LAST NAME	FIRST NAME	MIDDLE INITIAL	RESIDENCE (City and Either State or Foreign Country)
Lum	Stacey		Los Altos, California
Lee	Alice		Saratoga, California

TITLE OF INVENTION (280 characters max)

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

CORRESPONDENCE ADDRESS

Jennifer Pearson Medlin, Esq.

23859
PATENT TRADEMARK OFFICE

STATE	Georgia	ZIP CODE	30309	COUNTRY	USA

ENCLOSED APPLICATION PARTS (*Check All That Apply*)

- ☐ Provisional Application Title Page — *Number of pages* [ ]
- ☒ Specification, including claims and figures — *Number of pages* [12]
- ☒ Appendix — *Number of pages* [7]
- ☒ Credit Card Payment Authorization Form PTO-2038 for $80.00 for filing fee
- ☒ Other (Specify): Return Postcard

192479

EX2006

METHOD PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT (*Check One*)			
☒	A Credit Card Payment Authorization Form PTO-2038 is enclosed to cover the filing fees.	**FILING FEE AMOUNT**	**$80.00**
☐	The Commissioner is hereby authorized to charge filing fees and credit Deposit Account Number:		
☒	The Commissioner is hereby authorized to charge any additional fees which may be required in connection with the following or credit any overpayment to Deposit Account No. 14-0269.		

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

[X] No.

[ ] Yes. The name of the U.S. Government agency and the Government contract number are:

Respectfully submitted,

SIGNATURE_____ **Date** **10/21/03**

TYPED or PRINTED NAME: Jennifer Pearson Medlin **REGISTRATION NO. 41,385**
(*If Appropriate*)

NEEDLE & ROSENBERG, P.C.
Suite 1000
999 Peachtree Street
Atlanta, GA 30309
678-420-9300

EXPRESS MAIL NO. EL992020357US

CERTIFICATE OF EXPRESS MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as Express Mail Invoice No. EL992020357US in an envelope addressed to: MAIL STOP PROVISIONAL PATENT APPLICATION, Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450, on the date indicated below.

Michael Laird — 10/21/03 Date

192479

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.

Existing System 1a: CyberGatekeeper Remote

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.

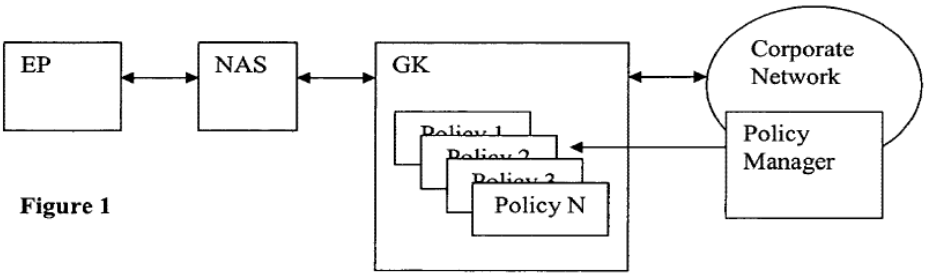


Figure 1

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.

By default, the GK is designed to prevent access to the corporate network if there are no rules granting access to the corporate network. If the EP's audit information complies with the policies, the GK lets the EP access the corporate network by setting a filter rule(s) that allows traffic from the EP to communicate with the corporate network.

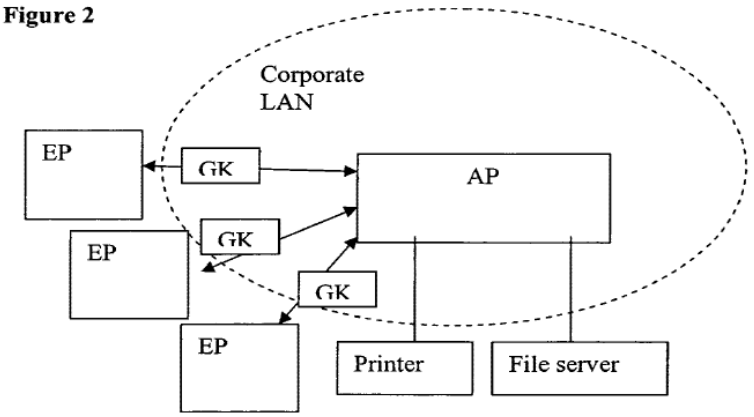
The GK continues to audit the EP regardless of whether the EP passed or failed the audit. This allows GK to allow or deny access if the EP configuration or applications change.

A disadvantage of this type of system is that network traffic between the EP and corporate network must pass through the GK to enforce access. If the network traffic between the EP and corporate network does not pass through GK, the filter rules would have no effect and would not be able to enforce access to the corporate network.

This is a problem when using a similar scheme to enforce access to the corporate network through an AP. Because the AP is part of the corporate network, much of the communications exchanged with an attached EP are to other EPs attached to the same AP. In such communications, the traffic remains inside the AP so the only external point where network traffic can be filtered for an EP is at each port of the AP.

Figure 2 shows how this would work. A large corporate network may use hundreds of APs, many of them with hundreds of ports, so this approach would be costly and impractical in the general case.

Figure 2



Another disadvantage to this system is that the EP must be capable of running an agent. Most NDs cannot run third party agents, and PCs whose operating systems are not supported cannot run the agents either.

Existing System 1b: VMPS

In a Cisco system, the proprietary VMPS protocol is used to program a switch to allow access by the EP to the corporate network upon authentication of the user identity. In this system, the AP uses the VMPS protocol require the user to enter a name and password which are authenticated by an authentication server.

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.

Existing System 1c: 802.1x

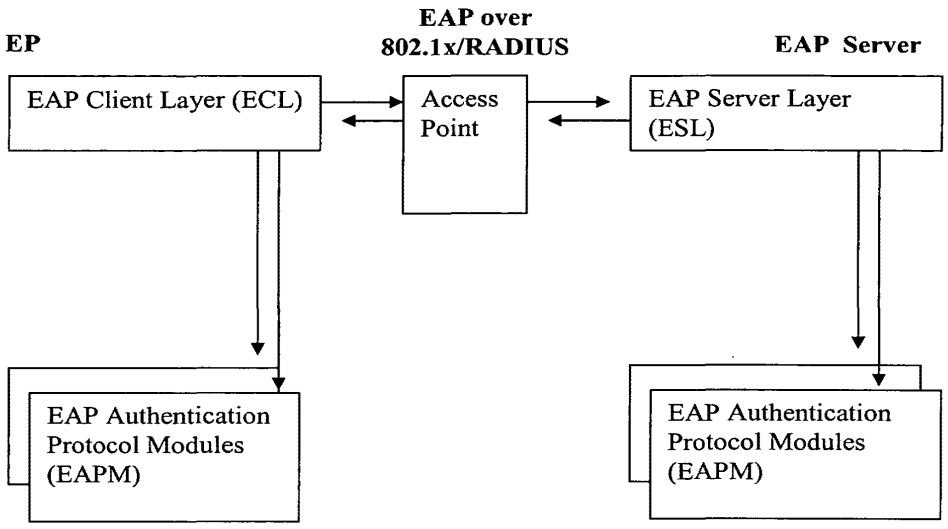
In a system using the 802.1x protocol, an authentication server enforces access by responding to 802.1x authentication requests. These requests originate from PCs that have 802.1x compliant client software that are forwarded through an 802.1x compliant AP. This system prevents users from accessing a network until they provide the proper authentication credentials, such as user name and password or a digital certificate.

In this type of system, the PC sends the authentication credentials, which are converted to 802.1x compliant EAP packets that are sent to the 802.1x compliant AP. The 802.1x compliant AP forwards the 802.1x EAP packets to an authentication server which verifies the credentials. Alternatively, the PC can send some or all of the authentication credentials automatically without user intervention.

The system optionally encrypts communications by using an EAP encryption protocol. This protocol runs first, then subsequent EAP authentication requests are embedded inside the EAP encryption protocol to ensure privacy. In network terminology, this technique is called "tunneling", whereby one protocol (the EAP authentication protocol) is embedded into another protocol (the EAP encryption protocol). After the authentication protocol has finished running, the encryption protocol also supplies a private key for encrypted communications for general traffic between the AP and EP.

A problem with this system is that it does not check whether or not the applications and configuration on the EP comply with an organization's security policies. This means that users whose EPs have security vulnerabilities or EPs that have been compromised (i.e. have been successfully attacked) can access the company network and potentially damage the network or other systems. Figure 3 shows the key components for this system.

Figure 3


EP
EAP over
802.1x/RADIUS
EAP Server
EAP Client Layer (ECL)
Access
Point
EAP Server Layer
(ESL)
EAP Authentication
Protocol Modules
(EAPM)
EAP Authentication
Protocol Modules
(EAPM)

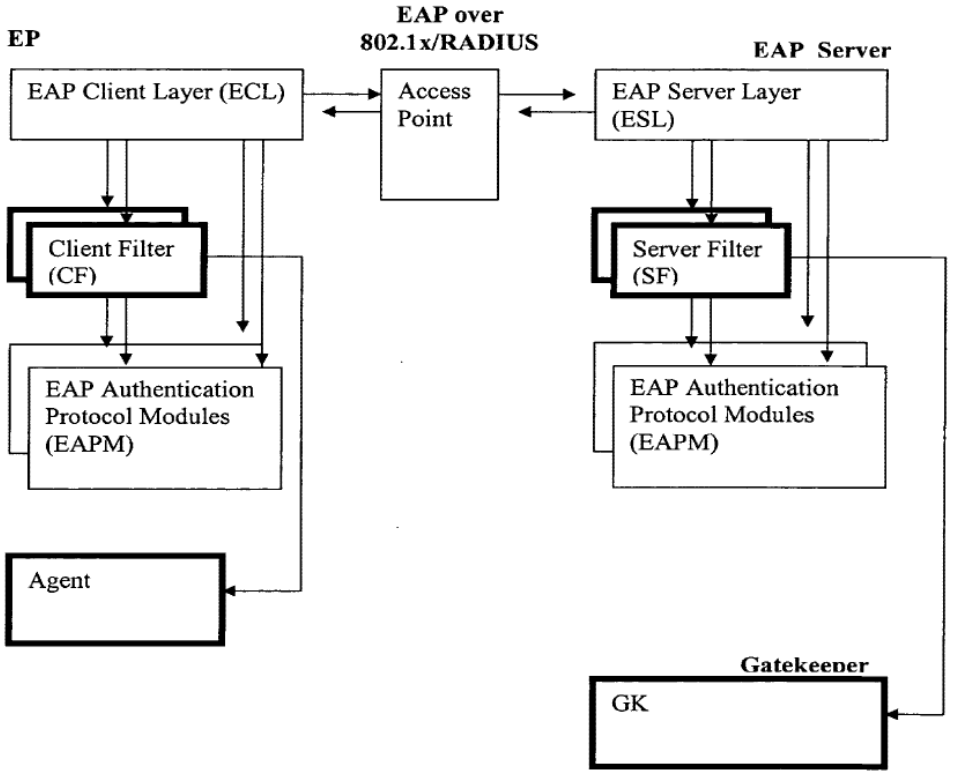
Invention

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.

Figure 4



The CF and SF APIs have APIs which correspond to the EAPM APIs. Therefore, the ECL or ESL can call the CF and SF instances corresponding to a particular authentication method as shown in Figures 5a and 5b. To the ECL and ESL, each instance of the CF and SF appears to be an EAPM which incorporates the functionality of the original EAPM prior to completion of the success response by the server EAPM.

Figure 5a: Client in Authentication State

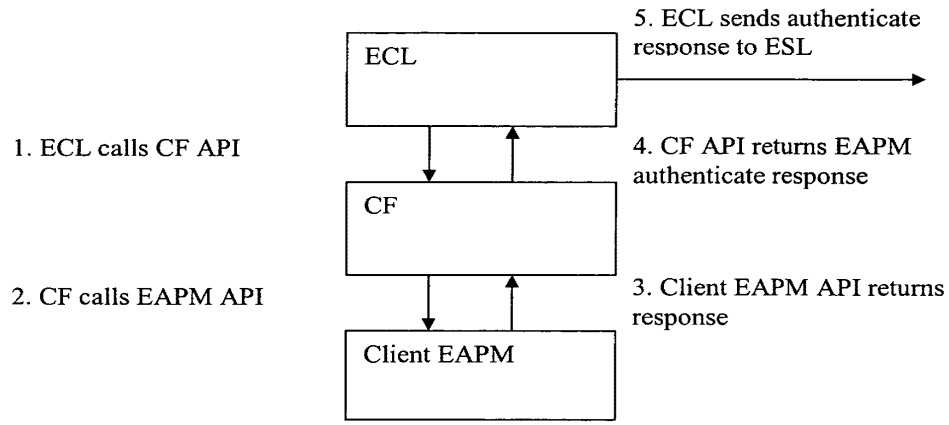
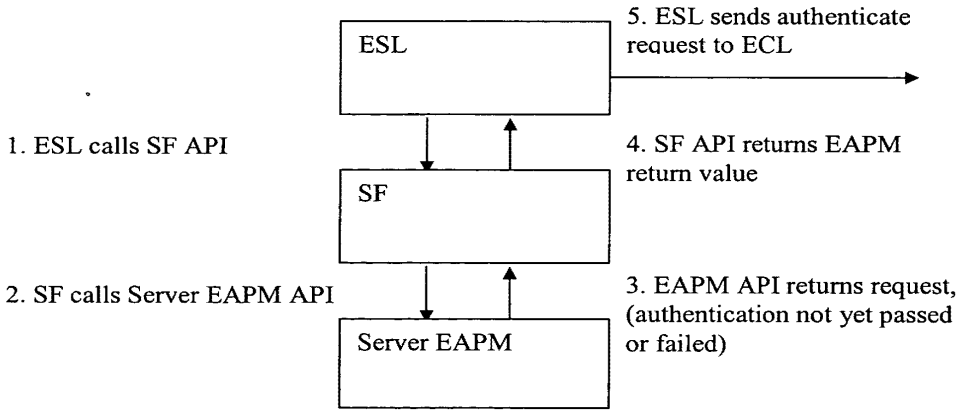


Figure 5b: Server in Authentication State



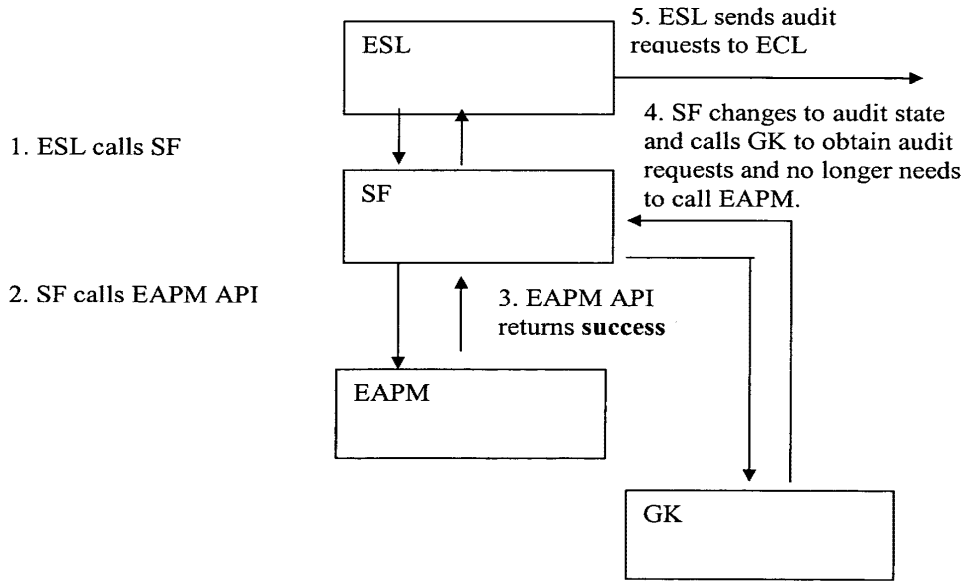
To use the invention, the ECL and ESL are configured to use the instance of the CF and SF corresponding to the desired authentication method. This authentication method corresponds to an authentication method supported by one of the EAPMs.

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.

Figure 6: Server Changing to Audit State



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

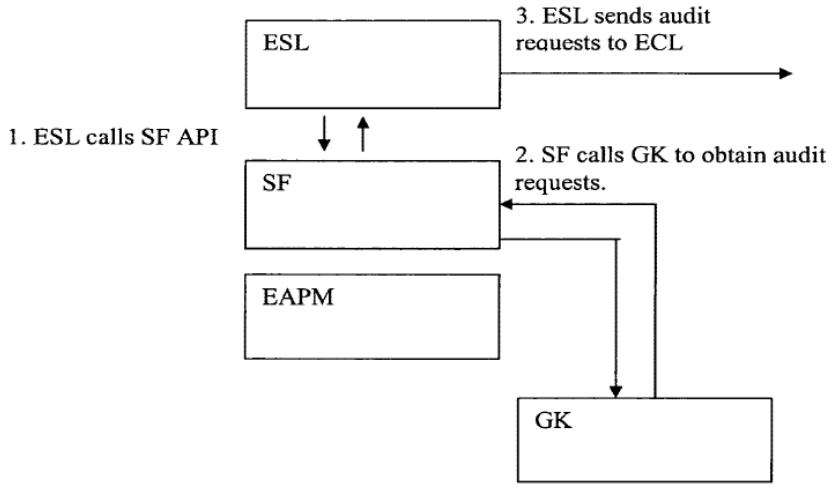
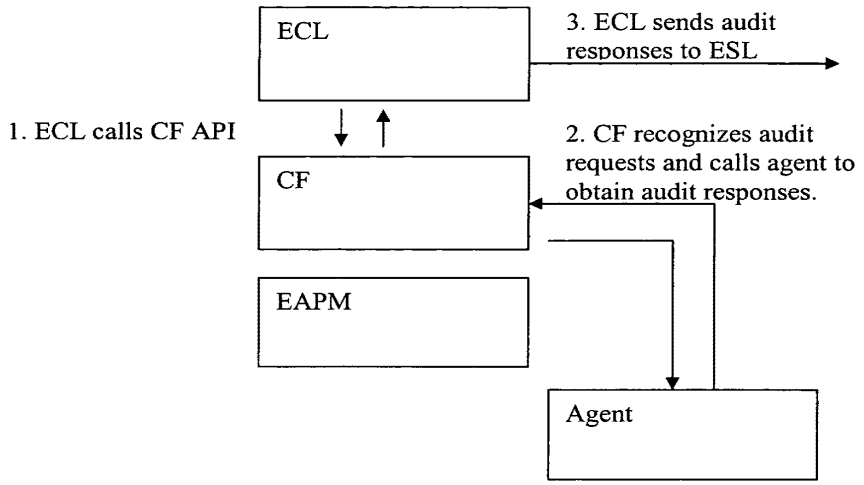


Figure 7b: Client Responding to Audit Requests



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.

Advantages of this invention are that:

1. The invention works with any AP that supports 802.1x. Additional protocols or interfaces are not needed to be compatible with this invention.

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.

APPENDIX

infoExpress Secure the last mile

CyberGatekeeper Enforcement Modes

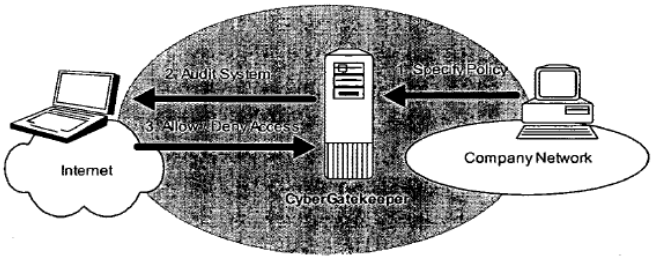
http://www.infoexpress.com

(c) 2003 InfoExpress, Inc. 1

infoExpress Secure the last mile

Inline Mode Simplified

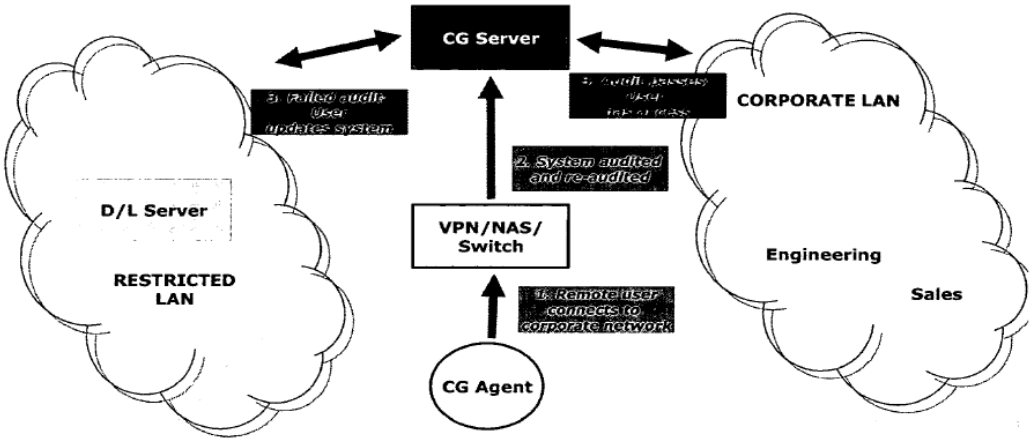
- DDefine acceptable configurations and applications
- AAudit remote system for compliance
- EEnforce access based on results of audit



(c) 2003 InfoExpress, Inc. 2

infoExpress Secure the last mile

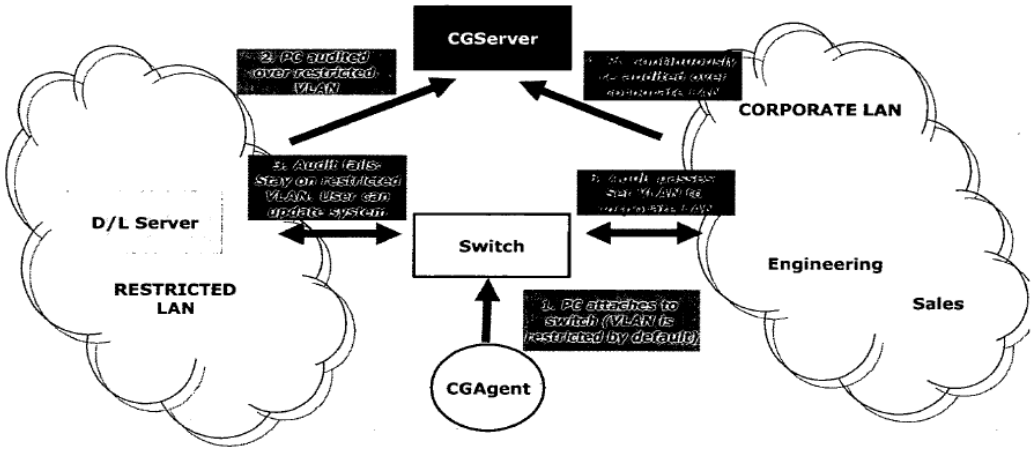
Inline Mode
Audit and normal traffic traverses CGS



(c) 2003 InfoExpress, Inc. 3

infoExpress Secure the last mile

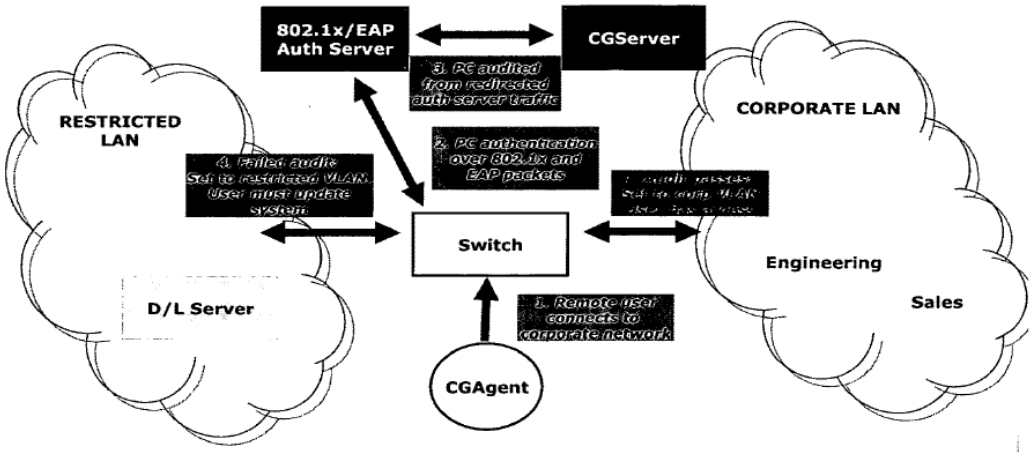
LAN Mode
Normal traffic does not traverse CGS



(c) 2003 InfoExpress, Inc. 4

infoExpress Secure the last mile

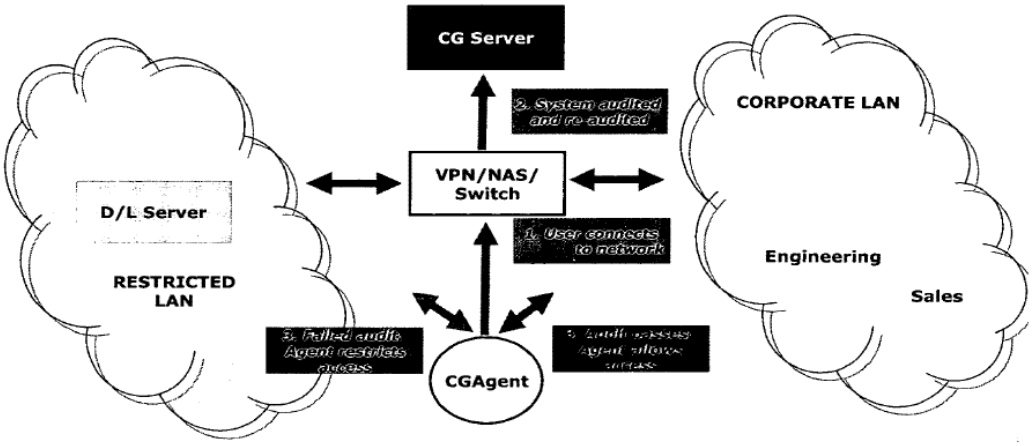
802.1x Mode
Normal traffic does not traverse CGS



(c) 2003 InfoExpress, Inc. 5

infoExpress Secure the last mile

Audit Mode
Client Side Enforcement



(c) 2003 InfoExpress, Inc. 6

PATENT APPLICATION SERIAL NO. _____

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE
FEE RECORD SHEET

10/24/2003 MMEKONEN 00000112 60513080
01 FC:2005 80.00 OP

PTO-1556
(5/87)

*U.S. Government Printing Office: 2002 — 489-267/69033