

ATTORNEY DOCKET NO. 09142.0001U1

1



PROVISIONAL APPLICATION FOR PATENT COVER SHEET

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

Docket Number		09142.0001U1		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		
TITLE OF INVENTION (280 characters max)					
GATEKEEPER INVENTIONS FOR CONTROLLING ACCESS TO A CORPORATE NETWORK					
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, figures and Abstract		Number of pages [14]			
☐ Drawings		Number of sheets []			
☒ Credit Card Payment Authorization Form PTO-2038 for \$80.00 for filing fee					
☒ Other (Specify): Return Postcard					



188118

Cisco v. InfoExpress
INFOEXPRESS
POPR
EX2005

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.		

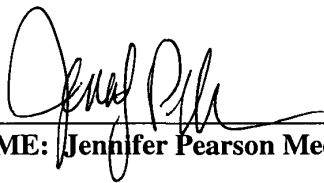
The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

[X] No.

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

Respectfully submitted,

SIGNATURE



Date

09/24/03

TYPED or PRINTED NAME: Jennifer Pearson Medlin

REGISTRATION NO. 41,385

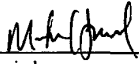
(If Appropriate)

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

EXPRESS MAIL NO. EL992020414US

CERTIFICATE OF EXPRESS MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as Express Mail Invoice No. EL992020414US 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

Date

9/24/03

**GATEKEEPER FOR CONTROLLING
ACCESS TO A CORPORATE NETWORK**

This 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 system which grants or denies access to the corporate network from end points.

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.

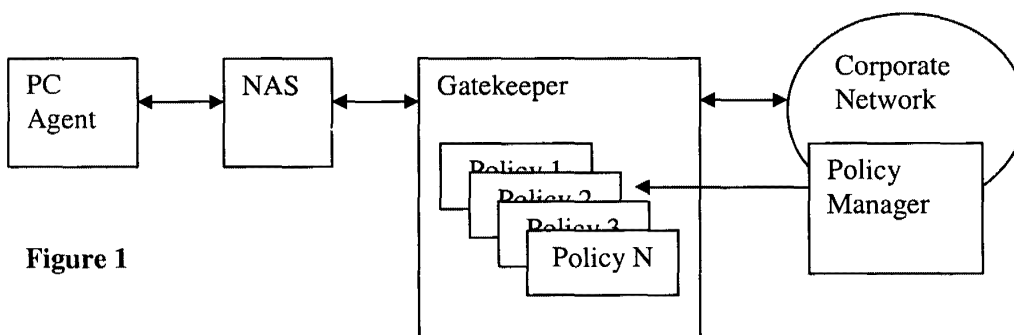
EP – End point which can be a PC or ND.

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.

System 1a

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.

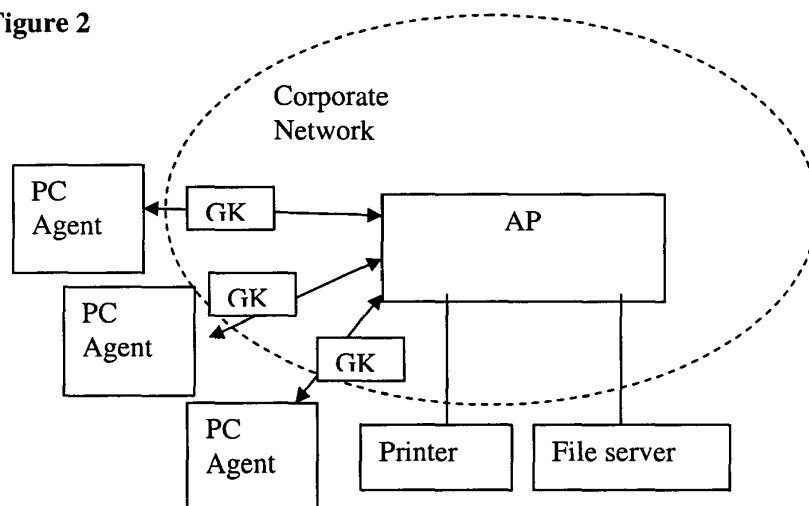
This is a problem when using a similar scheme to enforce access to the corporate network through an AP. Because the AP is part of the corporate network, much of the communications exchanged with an attached EP are with other EPs attached to the same

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 works. 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.

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.

Figure 2



System 1b

In another type of system, an AP can use a protocol to require user authentication before the EP can access the corporate network. In this type of system, the user or the EP itself must enter authentication credentials (e.g., a name and password) which are verified by an authentication server before access is granted.

In a Cisco system, the proprietary VMPS protocol can program a switch to allow the EP to access the corporate network after authentication of the user's name and password. When using the 802.1x, a standards based protocol, similar functionality is provided. In both cases, the EP is allowed access to the corporate network based on the user identity.

A problem with this system is that it does not check whether or not the applications and configuration on the user's system comply with corporate security policies. This means

InfoExpress Confidential

Author: Stacey Lum

that users whose EPs have security vulnerabilities or EPs that have been compromised (e.g., have been infected with a virus or trojan) can access the corporate network even when using such systems because the systems do not ensure that system configurations are correct before granting access to the corporate network.

Another problem is that both systems require the AP to support VMPS or 802.1x protocols. However, many existing APs do not support these protocols or may require expensive upgrades to support the protocols.

Invention

As in previous systems, policies are created by a central policy manager, which is connected to the corporate network. The policies are then transferred to one or more GKs on the corporate network which are responsible for enforcing access to the corporate network for one or more APs.

The GKs have the ability to assign a VLAN for attached EPs. For switches, the GK can set the VLAN for each port of the AP. For WAPs, the GK can set the VLAN associated with a specific EP on the wireless LAN.

One or more policies specify the audit criteria that must be met for EPs to access the corporate network, as well as which policies are applicable to the EP. Additionally, the VLAN settings which are used for the EPs meeting and failing audit criteria are stored in either the policy or configured on the gateway. The VLAN settings include: (i) a restricted VLAN to set for ports where EPs should be denied access, and (ii) optionally, a protected VLAN to set for ports when an EP should be allowed access.

Audit criteria include, but are not limited to, any combination of required and/or prohibited metrics for an EP. These metrics include, but are not limited to: applications running on the EP, configuration settings on the EP, identity of the user currently logged into the EP, system identity of the EP, operating system and patches used on the EP, network services running on the EP, addresses associated with the EP including IP and MAC, and the types of network packets received or not received from EPs.

The GK must obtain the metrics associated with the EP and the port to which the EP is attached to determine whether the EP meets the audit criteria. This information may be obtained in several ways:

- 1) An agent running on the EP can report information about the EP to the GK. Either the GK or the agent may initiate communications with the other, but information about the EP is passed to GK which is used to audit the EP. Information read by the agent and sent to the GK may include registry settings (for Windows), active or past processes, files, shared libraries, configuration files, date and time stamps of files, directories, users logged into the system, machine

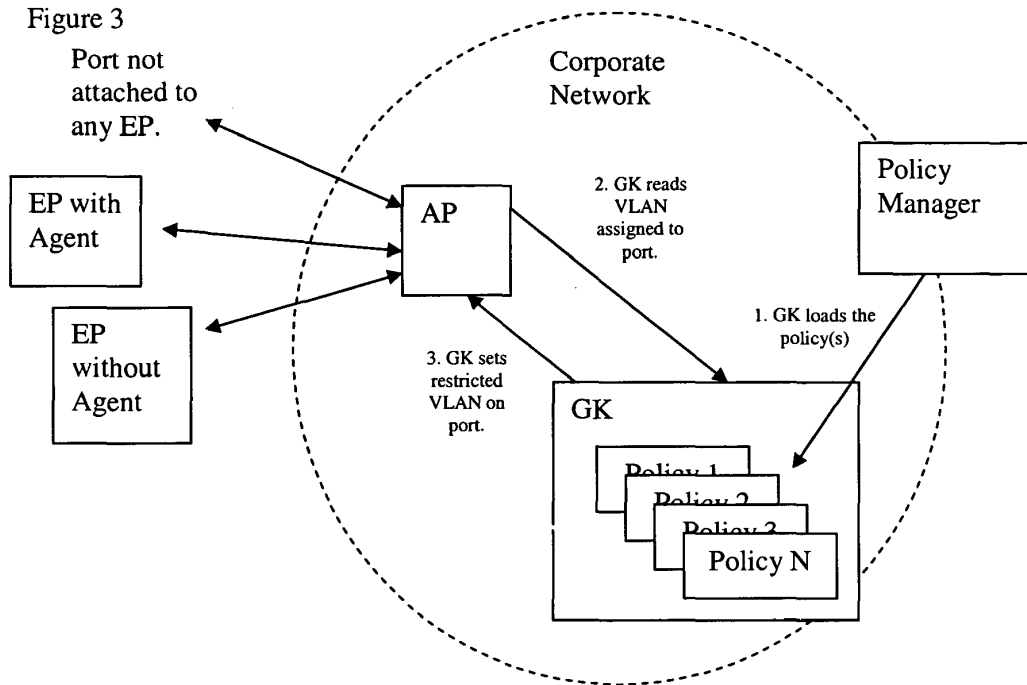
name, work groups or domains, host names, IP addresses, and other information about the EP.

- 2) The GK can read information from network equipment to which the EP is directly or indirectly attached, such as the AP or a router connected to the AP. For example, this information can be obtained by using SNMP, telnet or SSH to query the switch for MAC addresses and querying the routers in a similar manner to look up the corresponding IP address(es) associated with the MAC addresses.
- 3) The GK can probe the EP by sending specific packets to it. Based on examination of the response or lack of a response, the GK can determine information about the EP. The content of the probe packets is specified from a script or configuration file, and the response to the probe from the EP can be examined to determine whether it meets the audit criteria or not through a corresponding script or configuration file.

When an EP meets the audit criteria, the GK sets the VLAN on the corresponding port on the AP to the protected VLAN. This VLAN can either be the protected VLAN specified in the policy or configured on the GK, or the VLAN that was previously assigned to the port before GK programmed the port.

According to an exemplary embodiment, the GK first communicates with the AP to read which VLAN is associated with the port. If the VLAN for a port is not a restricted VLAN and not a VLAN previously set by the GK, the GK remembers the association between the port and the VLAN, noting that this VLAN is a protected VLAN for the port. Reading and setting the VLAN on the AP is performed using a protocol supported by the switch, such as telnet, SSH, or SNMP.

The GK then sets the port to the restricted VLAN. Setting the port to a restricted VLAN restricts access to the company network for any EP attached to the port. This operation may occur before the EP attaches to the port or immediately after an EP attaches to the port. See Figure 3.

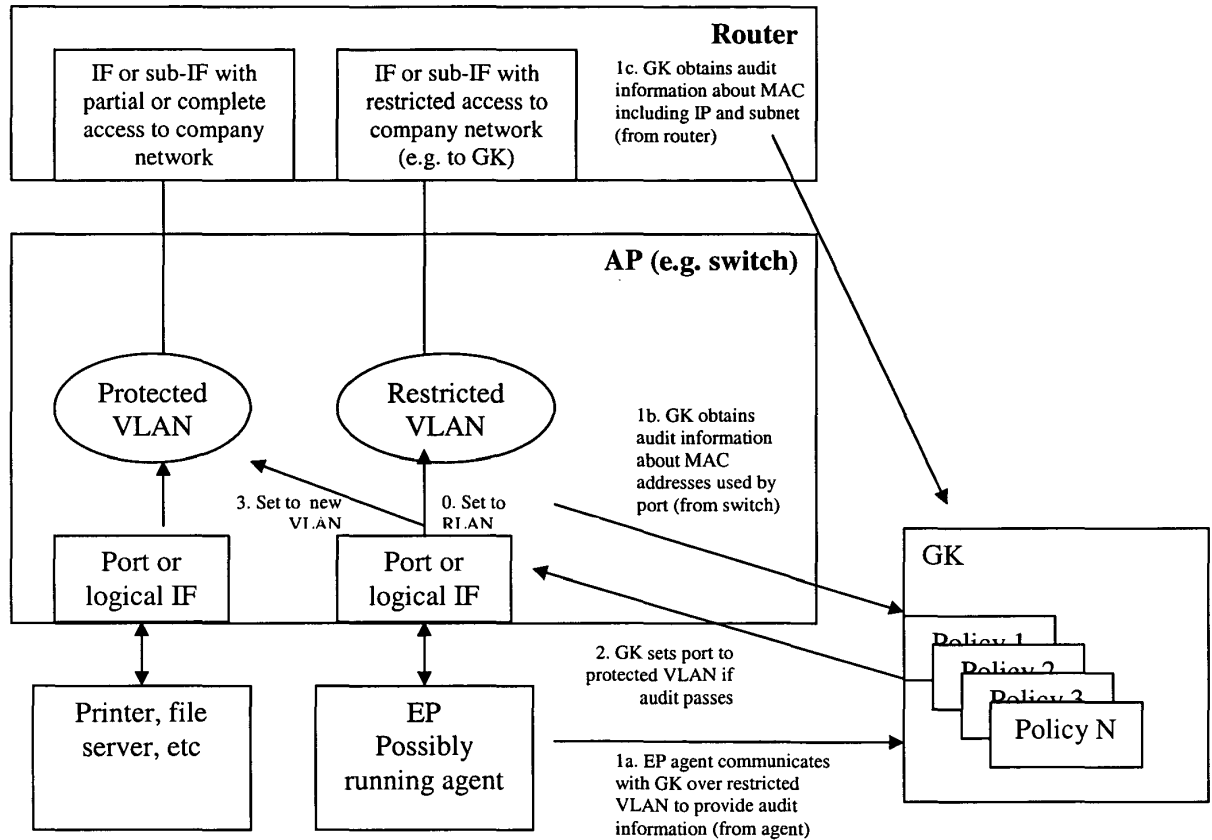


The GK then obtains information about any EP attached to the port to determine if it meets the audit criteria. If the audit criteria are not met, the GK leaves the port assigned to the restricted VLAN which limits access to the corporate network for any EPs attached to that port. See Figure 4.

If the audit criteria have been met, the GK assigns a protected VLAN to the port. The protected VLAN is the one specified in the policy or GK configuration, if present. Otherwise, the protected VLAN is the one noted previously, which was read before GK assigned a restricted VLAN.

A protected VLAN can provide full access to the corporate network or partial access by setting the access control list (ACL) on the router. By assigning different ACLs to the router interfaces for different protected VLANs, the varying degrees of access can be provided to the corporate network based on the VLAN assignment indicated in the policy.

Figure 4



Advantages of this invention are that:

1. An AP is supported whose VLANs can be set and read over the network. New protocols or interfaces for the AP are not needed.
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. An EP which is incapable of running an agent (such as a printer) or for which an agent is not available can still be allowed to access the corporate network because the gatekeeper can obtain audit information from the AP or routers to which the EP is attached.
4. The invention is highly scalable because a single GK can control many different ports and APs (i) from a different network, (ii) without directly connecting to the AP, and (iii) without requiring normal network traffic to traverse the GK.
5. If the routers used by the protected VLANs support ACLs, full or limited access can be provided to the corporate network based on the policy by setting the port to the VLAN whose router interface has the desired ACL.
6. Administrators can change VLAN assignments on the AP without informing the GK because the AP's protected VLANs are automatically read from the AP and remembered.

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

ATTORNEY DOCKET NO. 09142.0001U1

9

APPENDIX

InfoExpress Confidential

188332

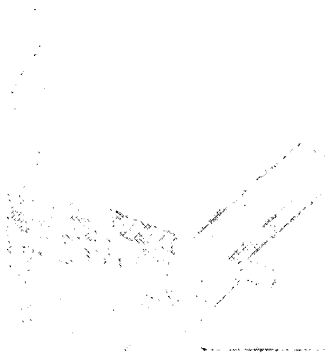
Author: Stacey Lum

InfoExpress

Secure the last mile

CyberGatekeeper Enforcement Modes

<http://www.infoexpress.com>



(c) 2003 InfoExpress, Inc.

1

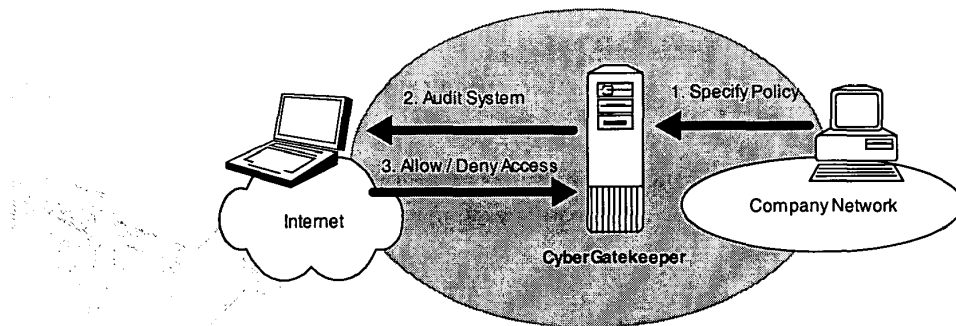
InfoExpress Confidential

Author: Stacey Lum

188332

Inline Mode Simplified

- Define acceptable configurations and applications
- Audit remote system for compliance
- Enforce access based on results of audit

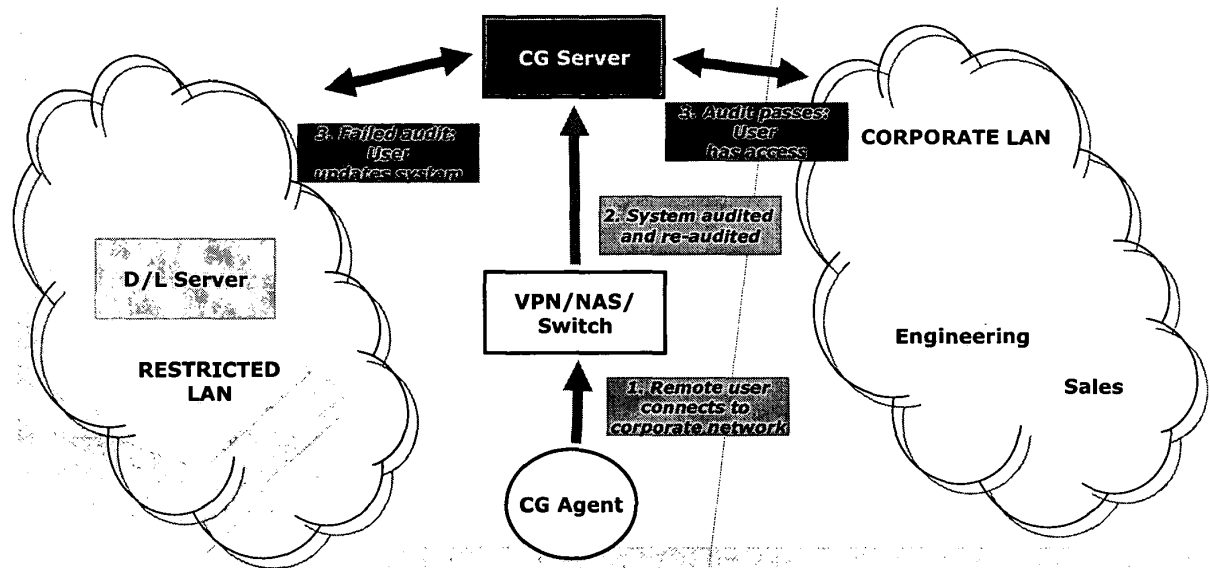


(c) 2003 InfoExpress, Inc.

2



Inline Mode Audit and normal traffic traverses CGS



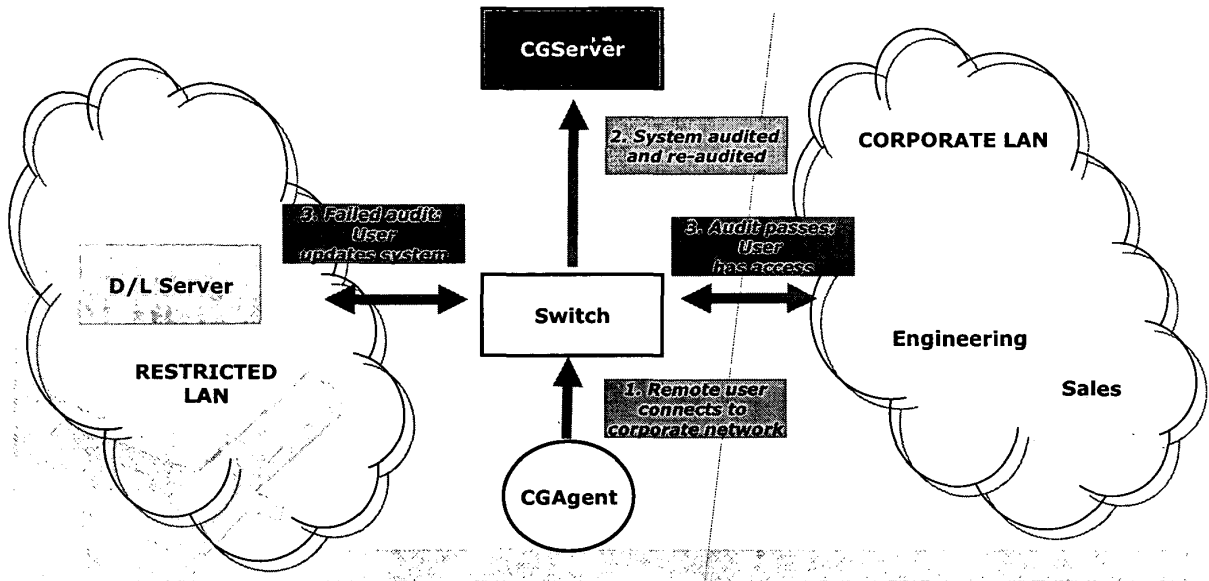
(c) 2003 InfoExpress, Inc.

3

Secure the last mile

LAN Mode

Normal traffic does not traverse CGS



(c) 2003 InfoExpress, Inc.

4

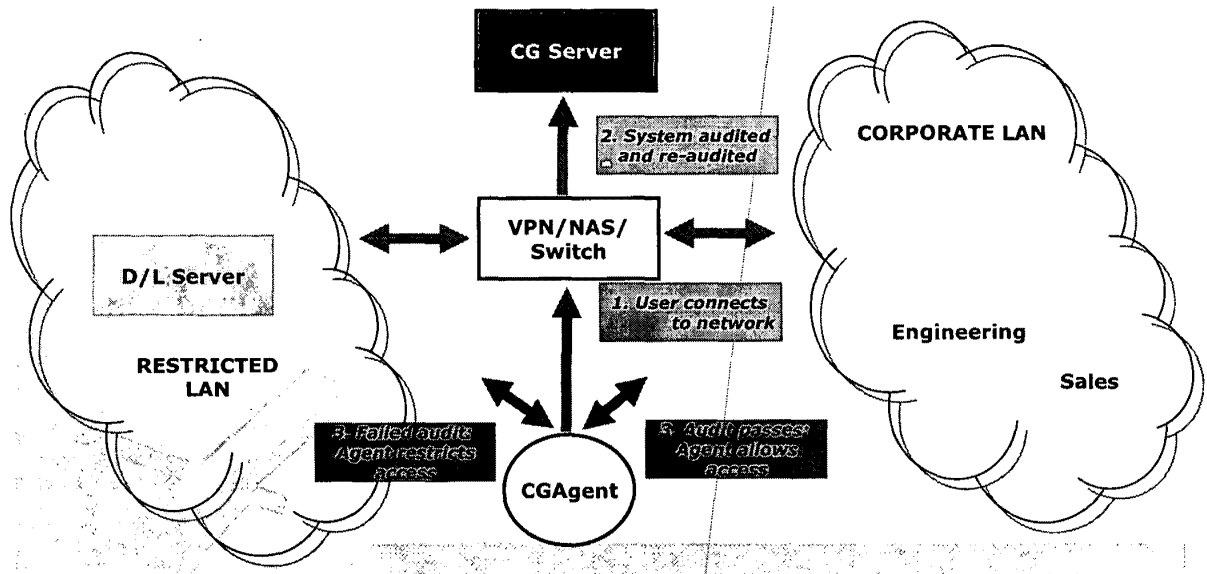
InfoExpress Confidential

Author: Stacey Lum

188332

Secure the last mile

Audit Mode Client Side Enforcement



(c) 2003 InfoExpress, Inc.

5

InfoExpress Confidential

Author: Stacey Lum

188332

PATENT APPLICATION SERIAL NO. _____

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

10/01/2003 ANABI1 00000014 60505582
01 FC:2005 80.00 DP

PTO-1556
(5/87)