



NETCLARITY presents...

A Case Study on **Auditor™**

Dynamically Detecting Laptops on Plug-in with Laptop Auditor

A NETWORK SECURITY & VULNERABILITY QUARANTINE SYSTEM (VQS™) CASE STUDY

A small bank approached NetClarity with a need to protect its network from potential hackers.

The bank's issue is one many banks and financial institutions of the 21st century can relate to—that financial advisors and mortgage loan officers from its affiliate brokerage firms and mortgage companies frequently visit with customers at the bank site and need to plug their laptops into the bank's network.

They may need to access data from the bank's database.

The bank's critical need is to deal with these units appearing on the network at unpredictable times. Any one of them could be bringing in viruses, worms, or Trojans, or allowing hacker access to the bank's critical data through exploitation of a vulnerability.

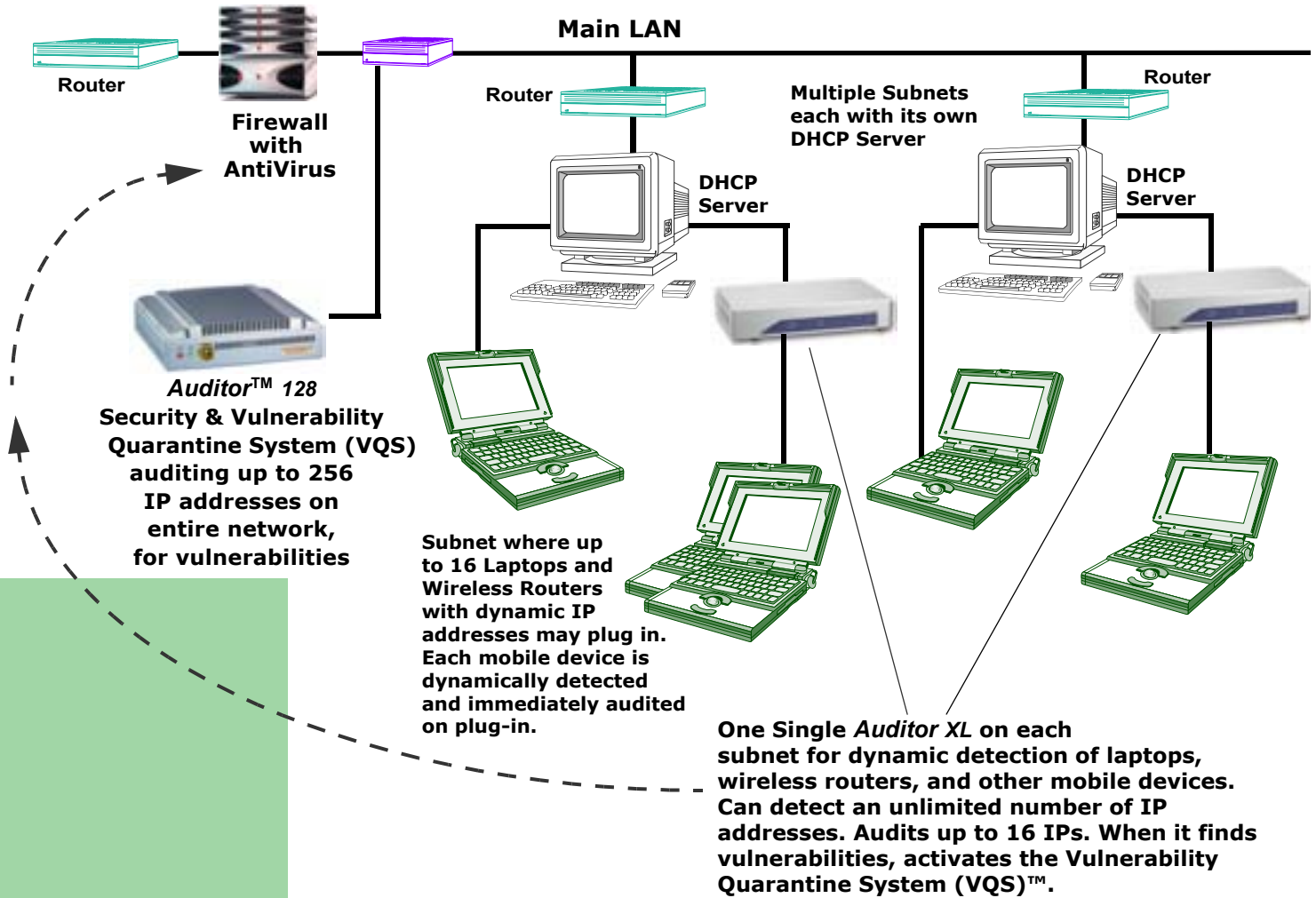
NetClarity engineers studied the network, which consists of a single main LAN where several subnets connect via routers.

Each of those subnets has its own DHCP server. Each device that connects to the subnet is dynamically

assigned an IP address by the DHCP server. **Auditor** immediately detects

new systems that plug into the network.

Network Security Solution for Bank with Multiple Laptops Frequently Plugging In at Unpredictable Times



The engineers explored the details of how many units might plug in to an individual subnet and the total number of units that would be on the network. They determined that each subnet would never exceed 16 IP addresses and that the entire network would never exceed 256 IP addresses.

Each unit on the network must be tested for vulnerabilities on a regular basis. It would be ideal to have the system that audits the network for vulnerabilities find the laptops as they randomly plug in and audit them.

Once a laptop plugs in, it too must be tested for vulnerabilities.

The solution NetClarity engineers devised is to have one **Auditor 128** audit the entire network on an on-going basis. It would be connected off the first switch inside the firewall and test the entire network for vulnerabilities on a regular basis.

To deal with the laptops visiting the network, NetClarity applied a special **Vulnerability Quarantine System™** that is available on every model of the **Auditor** appliance.

Each subnet at the bank would have its own single branch **Auditor XL** (also called the **Laptop Auditor** because of its ability to find visiting laptops) to run a constant dynamic detection process on each subnet.

The **Laptop Auditor** is designed to protect small branch offices or small subnets within a larger network. Its dedicated role in this situation is to dynamically detect laptops or other mobile devices immediately on plug-in to the network and then to audit those devices instantaneously. In that role it is key to protecting the network.

If the Laptop **Auditor** finds vulnerabilities on any device it detects, whether mobile or not, it quarantines the device using its **Vulnerability Quarantine System (VQS)™**. The **VQS** communicates with both firewalls and smart switches, allowing it to work in multiple network architectures.

At the bank, the **VQS** interacts with the firewall and directs it to quarantine any

vulnerable laptop by shutting down traffic to and from the device until it has been cleared to have access to the network.

The **VQS** also operates on the same principle on regularly audited systems, as it can quarantine any device on the network.

Quarantined systems (laptops or otherwise) remain shut out until the IT Manager directs the firewall to resume traffic to and from those nodes.

The **VQS** feature is compatible with several firewall brands and models, including Juniper, CyberGuard, Cisco, and Check Point. It also works with Cisco's intelligent Catalyst switches.

The bank is now secure in the knowledge that its constantly changing network is still locked down, despite laptops plugging in at random times. It is even protected from the possibility of a wireless router being connected to the network without authorization.

Officers of the bank receive regular reports on the vulnerability status of each networked device. These reports help form an audit trail for GLBA and SOX-404 compliance as well as for FDIC audits.

Auditor with its **VQS** system provide two areas of assurance to the bank—they make the bank network more secure and they help show the officers have exercised due care and due diligence in protecting confidential data housed in network systems.

Copyright © 2004-2005 PredatorWatch, Inc., d/b/a NetClarity. **Auditor™** and **VQS™** are trademarks of NetClarity. NetClarity is an IBM business partner.