Falsification Prevention and Protection Technologies and Products

Development of PC Quarantine System

By Nobuyoshi TANAKA,* Koji FUKUDA,* Hiroaki NAKADA* and Hiroki SHIMOKAWA†

ABSTRACT "Quarantine," new antivirus technology, has been getting increasing attention due to the recent emergence of harmful worms such as SQLSlammer, Blaster and Nachi. This technology is designed to prevent insecure PC's connect to enterprise network at border. NEC has worked on developing this technology for a while and has recently started to ship the "PC Quarantine System," integrated with the cyber attack protection system "CapsSuite V3.0," has various unique features which other vendors' products do not have. This paper outlines and describes the features of the "PC Quarantine System."

KEYWORDS **Quarantine, Antivirus, Cyber-Attack, Authenticated VLAN, Authenticated DHCP (Dynamic Host Configuration Protocol), Firewall, CapsSuite, VLANaccess, VitalQIP, IP8800**

1. INTRODUCTION

Antivirus software and firewalls have been rapidly introduced to the Japanese market due to the enormous damage caused by the worm CodeRed and the falsification of government home pages in 2000. It is said that introduction rates of antivirus software and firewalls are both over 90%. However, damage caused by virus was 3025 yen and still increasing according to the investigation by IPA (Information-technology Promotion Agency).

NEC has introduced CapsSuite, a total cyber-attack protection system that increases the security level of the IT of the business environment but it is very difficult to eradicate viruses by security management alone. According to NEC's internal research, the viruses have been introduced through mobile PCs even after security management has been enforced by CapsSuite (See **Fig. 1**).

In order to prevent virus infections through PCs that are not continuously under security control, new mechanisms should be introduced that checks the security level at the time a PC is about to connect to a corporate network and then approves the connection. This mechanism is called "Quarantine." (Some call it a self-defending network.)

2. FEATURE OF THE PC QUARANTINE SYSTEM

Some network equipment vendors and antivirus software vendors have also provided "quarantine" features. Unlike these sources, NEC introduces a unique concept, the "quarantine network," and also provides some variation in implementation patterns in order that customers can choose one that suits their requirements. Below, we describe the basic concept and features of NEC's quarantine network.

2.1 Typical Implementation of the Quarantine System

Figure 2 shows the typical implementation of the PC quarantine system.

Policy defined by Administrator discriminates the antivirus software version but some policies can also check active processes, DLL (Dynamic Link Library) versions and registry values. This form of implementation is common to VPN or SSL-VPN equipment and has the following weaknesses.

- Mainly protecting connections from outside.
- Cannot access an antivirus delivery system or a patch delivery system because it is disconnected from the corporate network.
- Policy is complicated.

2.2 NEC's Implementation of the "Quarantine Network"

NEC's PC quarantine system introduces a quarantine network that is separate from the corporate network, and does not disconnect target PCs from the

* Ubiquitous Software Division
†2nd Computers Software Division

network but dispatches them to a separate network, where users can make antivirus software up-to-date and download recent security patches (See **Fig. 3**).

The quarantine network requires methods which can switch networks. NEC provides three methods which can implement quarantine networks.

1) Authenticated VLAN (IP8800), authenticated DHCP (Dynamic Host Configuration Protocol)
2) Client firewall
3) Server firewall

These are described below.

2.3 Other Features

NEC also has following features other than the quarantine network.

- Quarantine is implemented based on a defined security level using CapsSuite, total cyber-attack protection system.
- Administrators do not have to generate complicated policy by using CapsSuite “Patch Delivery Information Package.”

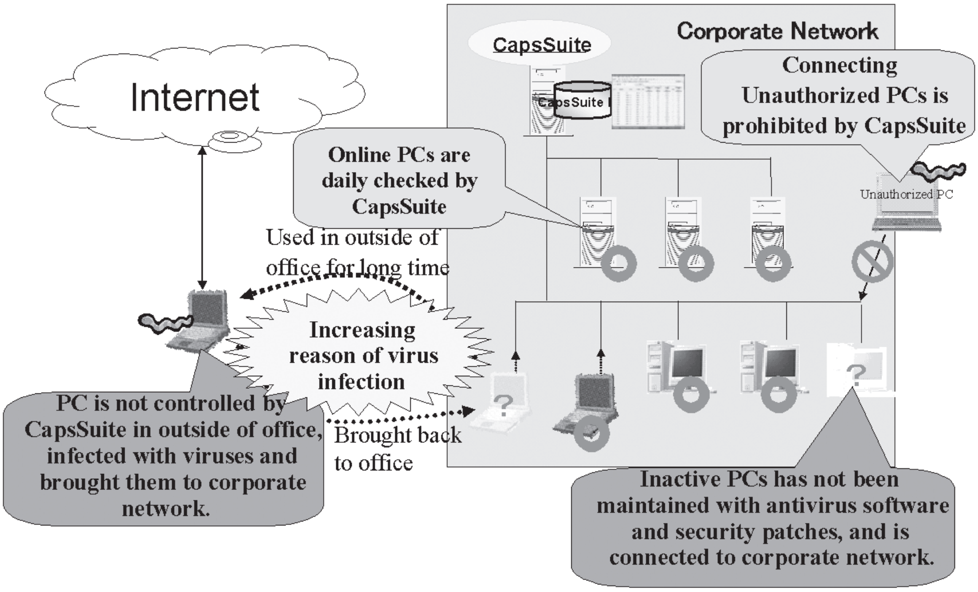
Internet
CapsSuite
Corporate Network
CapsSuite
Connecting Unauthorized PCs is prohibited by CapsSuite
Online PCs are daily checked by CapsSuite
Unauthorized PC
Used in outside of office for long time
Increasing reason of virus infection
Brought back to office
PC is not controlled by CapsSuite in outside of office, infected with viruses and brought them to corporate network.
Inactive PCs has not been maintained with antivirus software and security patches, and is connected to corporate network.
?
?

Fig. 1 Recent virus infection pattern.

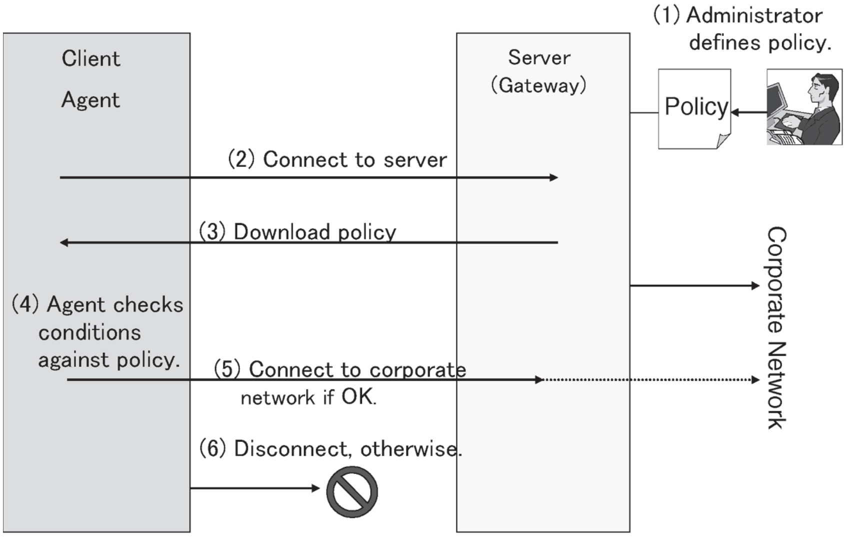
Client
Agent
Server
(Gateway)
(1) Administrator defines policy.
Policy
(2) Connect to server
(3) Download policy
(4) Agent checks conditions against policy.
(5) Connect to corporate network if OK.
(6) Disconnect, otherwise.
Corporate Network

Fig. 2 Typical implementation of quarantine system.

3. BRIEF OVERVIEW AND FEATURES OF EACH METHOD

This section describes a brief overview and features of the three methods that NEC provides. There are two reasons why NEC provides these three different methods.

- Customers can choose the best method based on their network requirements.
- Customers can choose the best method based on their quarantine targets and costs.

3.1 Authenticated VLAN Method

This method uses authenticated VLAN in order to switch between the quarantine and corporate networks. UNIVERGE IP8800 is used as authenticated VLAN equipment (See **Fig. 4**).

Figure 5 shows the flow chart of Authenticated VLAN Quarantine System.

① Authentication information (ID/password) is sent when client is logging into network.
② VitalQIP (Authenticated DHCP server) authenticate it.
③ VLANaccess asks CapsSuite Server for client security level after authentication is succeeded (CapsSuite DB is consulted).
④ VLANaccess configure IP8800 to switch the PC to the VLAN1 (Quarantine Network) in case that PC's security level does not comply with the required security requirements; and to VLAN2 in case that PC's security level does comply with the requirements.
⑤ The PC is connected to a Corporate Network in case it is switched to VLAN2 in Step ④.
⑥ The security level of the PC is checked again, required patches are downloaded and applied in the Quarantine Network, and the PC is rebooted in the case of a switch to VLAN1 in Step ④. CapsSuite DB will be updated once the patches are applied properly, which allows the PC to be connected to the Corporate Network at the next login.

As described, the PC is allowed to connect only to the Quarantine Network until the patches are up-to-date. Since it would be too exacting if the PC were always dispatched to the Quarantine Network right after a new patch is registered to CapsSuite, the administrators can configure it so that the system gives a little allowance to end users before starting the quarantine. We recommend the following configuration.

- When a certain time is passed after a new patch registration (e.g. one week).
- When a virus or a worm appears, which uses vulnerabilities the patch is fixed.

There are failsafe and operation functions in order to prevent the problems where PCs could not connect to the Corporate Network because of CapsSuite DB

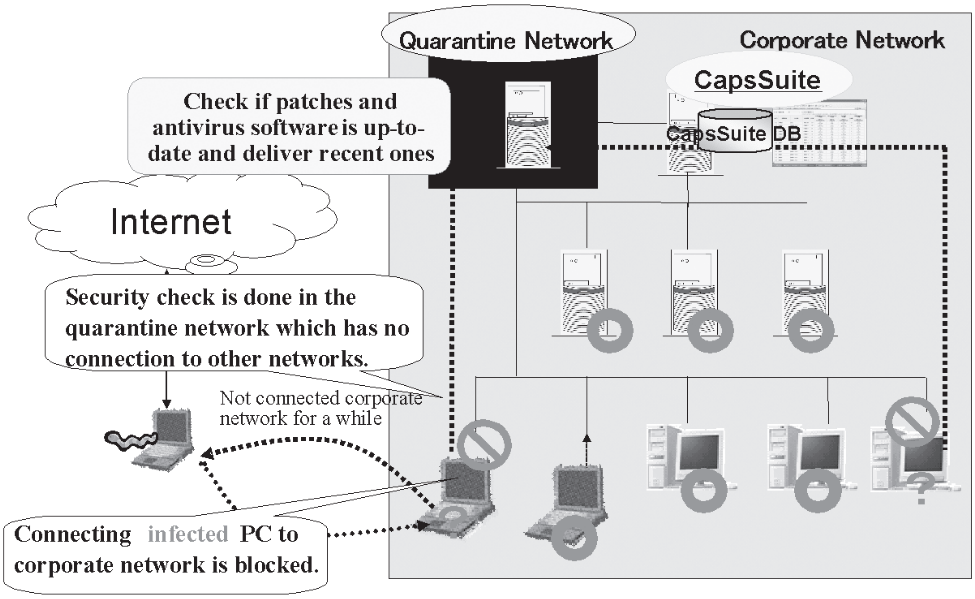
Quarantine Network
Corporate Network
CapsSuite
CapsSuite DB
Check if patches and antivirus software is up-to-date and deliver recent ones
Internet
Security check is done in the quarantine network which has no connection to other networks.
Not connected corporate network for a while
Connecting infected PC to corporate network is blocked.

Fig. 3 Quarantine network.

failure and/or Quarantine Server.

- Server failover.
- Temporary suspension of quarantine system.
- Quarantine exemption for a specific machine.

This method requires UNIVERGE IP8800 as a switch but may utilize other switches with small restrictions instead.

- Switches should have a secondary addressing

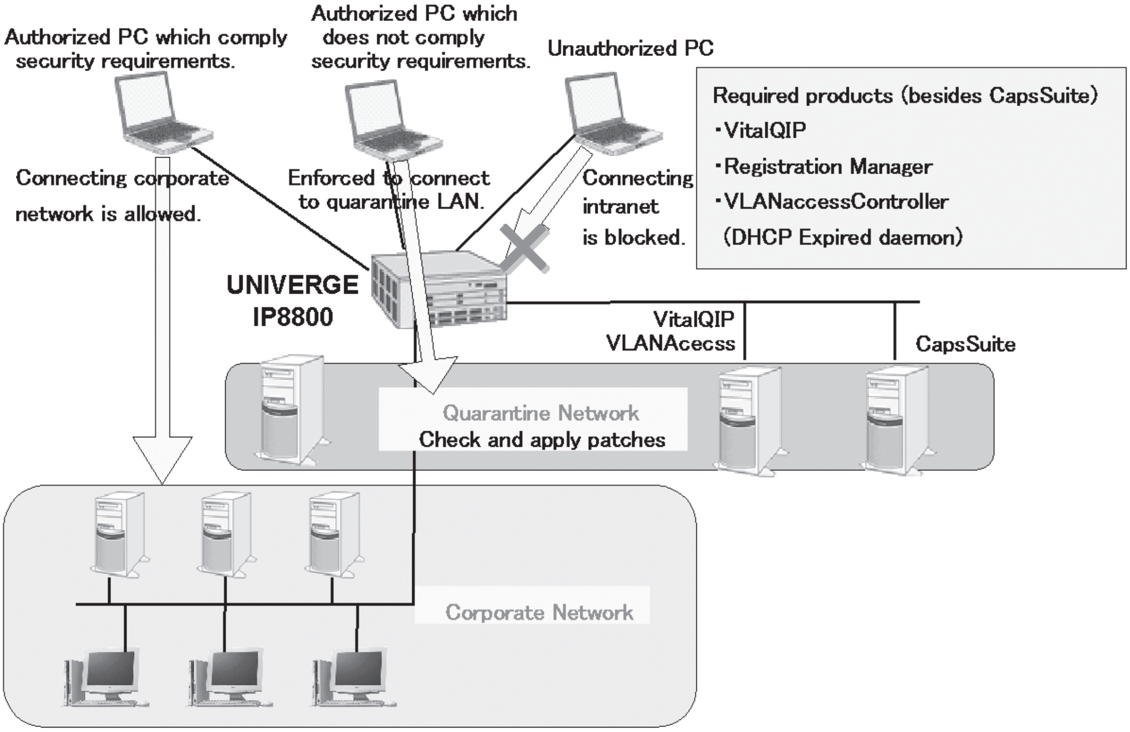
Authorized PC which comply security requirements.
Authorized PC which does not comply security requirements.
Unauthorized PC
Required products (besides CapsSuite)
・VitalQIP
・Registration Manager
・VLANaccessController
(DHCP Expired daemon)
Connecting corporate network is allowed.
Enforced to connect to quarantine LAN.
Connecting intranet is blocked.
UNIVERGE IP8800
VitalQIP VLANAcecss
CapsSuite
Quarantine Network
Check and apply patches
Corporate Network

Fig. 4 Authenticated VLAN method.

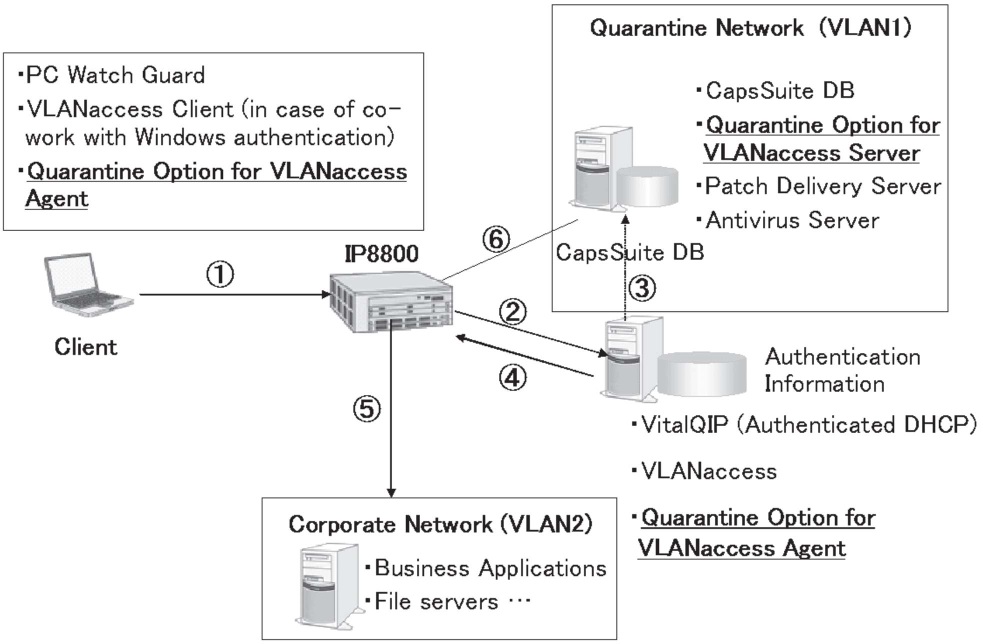
Quarantine Network (VLAN1)
・CapsSuite DB
・Quarantine Option for VLANaccess Server
・Patch Delivery Server
・Antivirus Server
CapsSuite DB
・PC Watch Guard
・VLANaccess Client (in case of co-work with Windows authentication)
・Quarantine Option for VLANaccess Agent
Client
IP8800
①
②
③
④
⑤
⑥
Authentication Information
・VitalQIP (Authenticated DHCP)
・VLANaccess
・Quarantine Option for VLANaccess Agent
Corporate Network (VLAN2)
・Business Applications
・File servers …

Fig. 5 How the authenticated VLAN method works.

feature, by which they can assign multiple IP addresses to a single port.

- Cannot be used as authenticated VLAN. For Authenticated DHCP only.

3.2 Client Firewall Method

This method switches between the quarantine network and corporate network by changing client firewall policy automatically, therefore, realizes a quarantine network independent of the physical network structure (See **Fig. 6**).

① Client agent configures client firewall [Symantec ClientSecurity, (SCS)] via Policy 1, which limits accessible outbound policy to the Quarantine network (XX.XX.XX.XX). The PC can only access Quarantine Network at this moment.

② Client agent connects to server agent and asks for security condition of client.

③ Server agent consults in CapsSuite DB and responds to client.

④ Client agent switches client firewall policy to Policy 2 if this condition is up-to-date. Policy 2 expands accessible outbound policy to Corporate Network (YY.YY.YY.YY). If the result of Step ③ is not up-to-date, recent patches are applied in the Quarantine Network, the security conditions are checked again, and finally the policy is switched to Policy 2 automatically because the security conditions should be up-to-date.

⑤ PC can access the Corporate Network once SCS switches policy to Policy 2.

As described above, there are several merits with the client firewall method.

- Virtual quarantine network can be implemented without any changes in the existing network structure.
- Network connection independent. This method can apply quarantine both for the intranet LAN connection and for an outside connection such as VPN, dial-up.
- Antivirus capability will increase by using client firewall.

However, only Symantec SCS can be used for this method.

3.3 Server Firewall Method

Unlike other methods, server firewalls (ServerW@ll) are placed in all of the servers to be protected. Firewalls will give access permission to PCs which pass the quarantine test (See **Fig. 7**).

① End users who want a server allocation have to check in ServerW@ll Authentication Server through ServerW@ll Client Agent.

② ServerW@ll Authentication Server checks the information sent from client agent, and makes

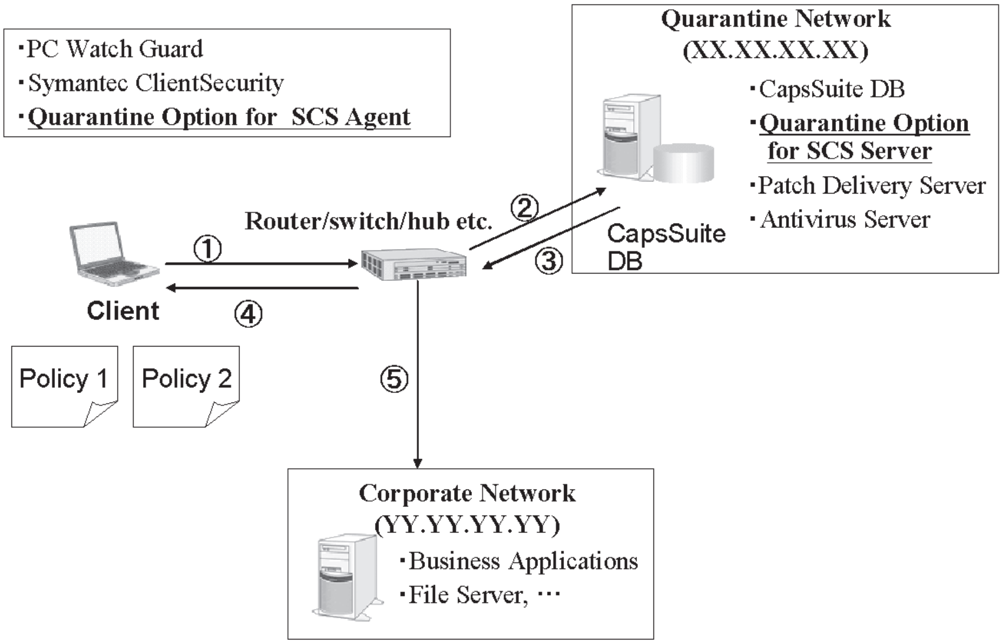

Fig. 6 Flow of Client Firewall Quarantine System.

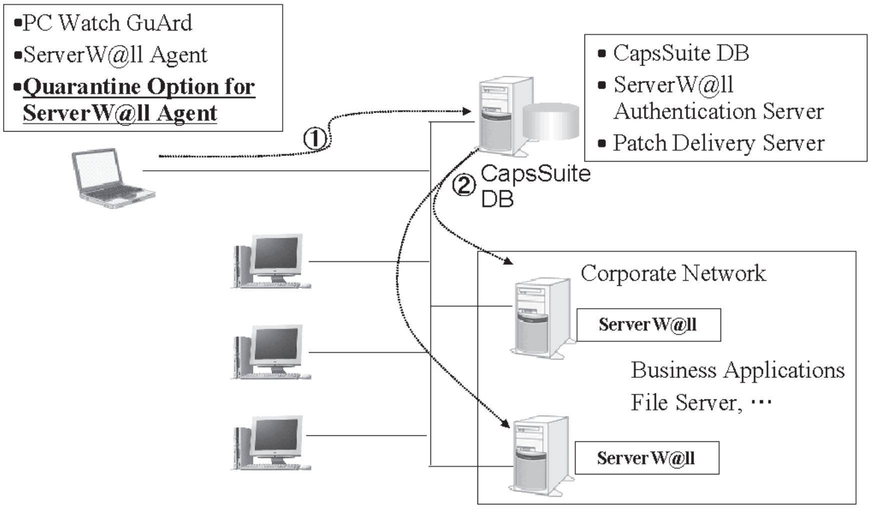

Fig. 7 Flow of the Server Firewall Quarantine System.

ServerW@ll inbound policy allow access from client.

As described above, there are several merits with the server firewall method.

- Network independent.
- Antivirus capability will increase by putting server firewall into servers where recent patches cannot be applied.
- Inexpensive compared with other methods.

However, this method cannot protect clients. There is a scale limitation, 100 servers per 5,000 clients.

4. CONCLUSION

Mobile PCs are increasingly becoming popular owing to the trend towards the global society. On the other hand, maintaining the security levels of these PCs becomes more and more critical with regard to cyber-attack protection. NEC will enhance quarantine solutions for various IT environments such as the wireless LAN system and the IEEE802.1X Authentication system. Also, the security requirements upon which quarantine system is based should include not only patches/antivirus measures but also information leakage protection capabilities.

Received January 31, 2005

* * * * * * * * * * * * * * *

Nobuyoshi TANAKA is Senior Manager of Security Group, Ubiquitous Software Division, NEC Corporation. He joined NEC in 1984.

Koji FUKUDA is Engineering Manager of Security Group, Ubiquitous Software Division, NEC Corporation. He joined NEC in 1982.

Hiroaki NAKADA is Assistant Manager of Security Group, Ubiquitous Software Division, NEC Corporation. He joined NEC in 2000.

Hiroki SHIMOKAWA is Assistant Manager, i-Office Server Group, 2nd Computers Software Division, NEC Corporation. He joined NEC in 1987.

* * * * * * * * * * * * * * *