H3C
IToIP Solutions Expert

H3C Wireless EAD Solution

I. Background

Nowadays many medium- and large-scale enterprises have deployed wireless local area networks (WLANs). The WLAN mode becomes a more and more important access means. The user terminals using wireless access, however, always move and are often beyond the monitoring of enterprise network administrators. Therefore, an increasing number of security issues arise with such user terminals.

In today's network environments, new security threats keep emerging and viruses are taking its way, often causing system down and network crash to incur severe losses to enterprises. In an enterprise network, the security status of any terminal will directly affect the security of the entire network. Terminals that do not conform to enterprise security policies are vulnerable to attacks and virus infection. If a terminal is infected by viruses, it will keep attempting to get the next victim in the network and make the victim also virus-infected. In a network without security protection, ultimately the entire network may be down with all terminals failing to normally work.

Ensuring that the security status of all terminals in the network conforms to enterprise security policies is a challenge to every network administrator. It takes time and effort for an administrator to search, isolate, and repair terminals that do not conform to security policies. More often, a big gap exists between enterprise security policies and terminal security implementation.

H3C Endpoint Admission Defense (EAD) solution is a part of H3C integrated WLAN solution for carriers. It can cooperate with wireless APs and ACs in the WLAN environment to implement endpoint admission control for wireless access users through authentication and to forcibly exercise enterprise security policies, so as to strengthen the active defense ability of network terminals, prevent dangerous and fragile terminals from accessing the network, and control the flooding of viruses, thus effectively meeting customers' secure wireless access requirements. This end-to-end security protection system can implement security policies in the terminal access layer and thus greatly improves the security of the entire network.

II. Wireless EAD Solution

In the wireless EAD solution, the iNode client supports unified authentication and can complete wireless authentication and security authentication at one time, thus facilitating deployment and use. In the wireless EAD solution, in addition to checking the user name and password of a user with a legal identity, the system also checks whether the user meets security policy requirements, including whether any antivirus software has been installed, whether the virus database has been upgraded, and whether necessary system patches have been installed. For a user that has passed both identity authentication and security authentication, the EAD system will allocate certain network access rights to the user according to the predefined policies, so as to prevent unauthorized network access and attain the effect of hard isolation.

Figure 1-1 shows the networking diagram of the wireless EAD solution.

Figure 1-1 Networking structure of the wireless EAD solution

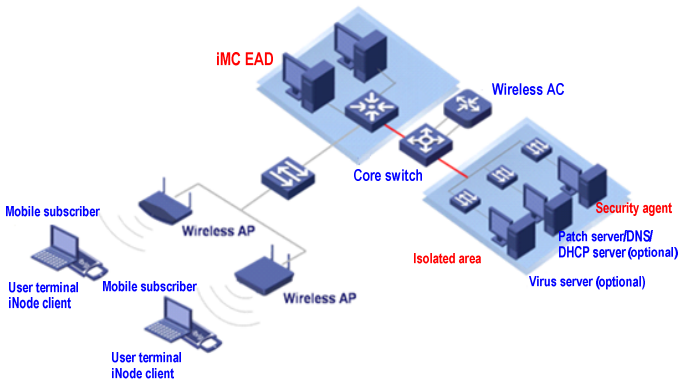
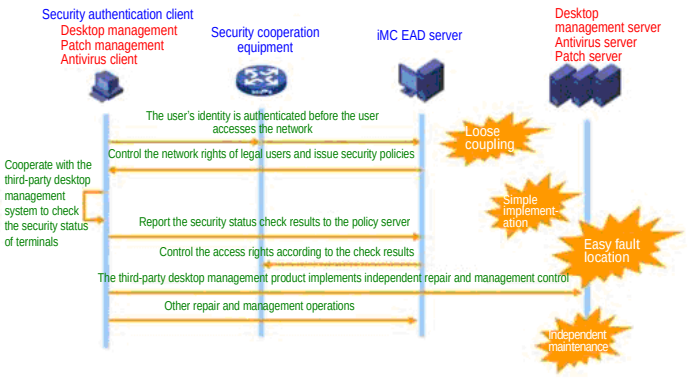


Figure 1-2 shows the service procedure of the EAD solution, which comprises four steps.

Figure 1-2 Service procedure of the EAD solution



III. Wireless EAD Solution

Step 1

A user terminal attempts to access the network. The user needs to pass user identity authentication via the security client. If the user is illegal, its access request will be denied.

Step 2

If the user is legal, it will be requested to perform security authentication. The security policy server verifies whether the security status of the user terminal conforms to the pre-defined security policies based on the user account, including whether the patch version and the virus database version are correct, whether the software installation is allowed, and whether any proxy server is used on the user terminal. If the security status of the user does not conform to the pre-defined security policies, the user will be placed by the security cooperation equipment to the isolated area.

Step 3

The user placed in the isolated area can upgrade the system patches and the virus database, uninstall illegal programs, and cancel the proxy settings, till its security status conforms to the pre-defined security polices.

Step 4

After the user's security status conforms to the pre-defined security policies, the user will implement the security settings issued by the security policy server. The security cooperation equipment provides identity-based network services.

As can be seen from the basic functions and operating principles of EAD, the EAD solution integrates terminal security measures (terminal virus prevention, patch repair, etc.) and network security measures (network access control, access rights control, etc.) in an interactive security system. By checking, isolating, repairing, managing, and monitoring network access terminals, it changes the entire network from passive defense to active defense, from single-point defense to comprehensive defense, and from scattered management to centralized policy-based management, thus improving the entire ability of the network to defend against emerging security threats such as worm viruses.

III. Advantages of the Wireless EAD Solution

u Based on Wireless EAD

The wireless EAD function can be implemented through cooperation between the wireless EAD client, the wireless AC, and the EAD policy server. The solution is applicable to networking scenarios with wireless access only and networking scenarios with both wired and wireless access.

u Complete Security Status Evaluation

The EAD client can perform security check, including checking the virus database version, patches, installed applications, the proxy server, and dialup settings. It can also be used with mainstream desktop security products in the industry such as Microsoft SMS, LANDesk, and BigFix, and can cooperate with the products of mainstream antivirus software vendors both home and abroad.

u Role-Based Network Authorization

The EAD system can issue pre-configured access control polices to the security cooperation equipment according to the terminal user role to normalize the network use behaviors of the user based on the rights of the user role.

u Extensible and Open Solution

The EAD solution provides an extensible and open framework for customers and thus protects the existing investment of customers to the utmost extent.

u Flexible Deployment

The EAD system treats different users with different security policies configured by the network administrator. Different security check and processing modes, including the monitoring mode, the alert mode, the isolation mode, and the disconnection mode, are customized for different users. In addition, the EAD solution supports flexible network reconstruction and the silent installation of the client.