H3C
IToIP Solutions Expert

H3C EAD Intranet Control Solution

I. Overview

Is your intranet vulnerable to virus flooding? Are you helpless when your employees access external networks by illegally setting up a proxy server on their PCs? Do you want to change the fire rescue mode?

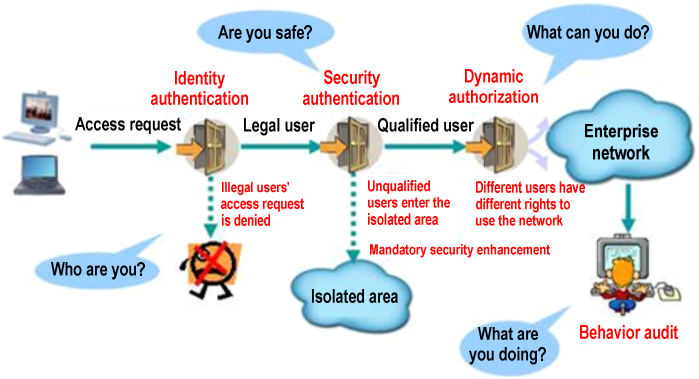
II. PC Management Problems

In an enterprise network, users may not timely upgrade the system patches and virus database on their terminal PCs. They often illegally set up a proxy server, access external networks without prior permission, and misuse forbidden software. Once fragile user terminals access the enterprise network, potential security threats quickly spread in a wider range and thus the network use may be out of control. Guaranteeing the security of user terminals, preventing security threats from intruding the network and effectively controlling the network access of users are the precondition for guaranteeing the secure running of an enterprise network as well as an issue to be urgently solved by enterprises.

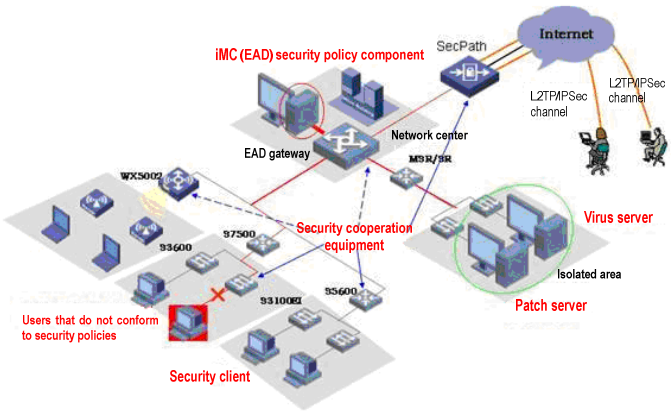
III. Same Solution

In essence, network security is a management issue. Aiming to guarantee user terminals' secure network access, H3C End user Admission Domination (EAD) solution integrates network access control and terminal security products to forcibly exercise enterprise security policies on user terminals accessing the network through interaction among the intelligent client, the security policy server, the network equipment, and the third-party software. The solution can strictly control the network use behaviors of terminal users and can effectively strengthen the active defense ability of user terminals, thus offering an effective and easy-to-use management tool for enterprise network administrators.

Before a user accesses the network, the EAD system authenticates the identity of the user. After the user passes the identity authentication, security authentication is performed on the user terminal. The system performs security check according to the security policies customized by the network administrator, including the virus database updating status, the system patch installation, and the software blacklist or whitelist. Then the EAD system authorizes and controls the user's network access according to the security check results. After passing the security authentication, the user can normally use the network. At the same time, the EAD system audits and monitors the running status and network use behaviors of the user terminal. The following figure shows the procedure of user access authentication according to the EAD solution.



The following figure shows the networking model, which comprises the iNode intelligent client, the security cooperation equipment, the iMC security policy server, and third-party servers.



iNode intelligent client: A user access terminal on which H3C iNode intelligent client software is installed to initiate identity authentication and check security policies.

Security cooperation equipment: switches, routers, VPN gateways or other equipment in the user network. The EAD solution provides flexible and diversified networking schemes. The security cooperation equipment can be flexibly deployed in various layers of the network according to the actual needs. For example, the security cooperation equipment can be deployed in the access layer or convergence layer of the network.

iMC (EAD) security policy component: A reachable route must exist between this component and the security cooperation equipment. This component issues security policies to the client, receives and audits the security policy check results from the client, and sends network access authorization commands to the security cooperation equipment.

Third-party servers: patch servers, virus servers, and security agent servers deployed in the isolated area. When a user has passed the identity authentication but fails to pass the security authentication, the user will be placed in the isolated area and can access only the third-party servers in the isolated area to perform security repair till the user meets the security policy requirements.

IV. Typical Deployment

LAN EAD Solution

User terminals usually access an intranet via a switch. The EAD system interacts with the switch to forcibly check the virus database and system patches of the user terminal so as to reduce the risk of virus flooding. The EAD system also forcibly implements security policies on users accessing the network so as to prevent security threats coming from the intranet.

WAN EAD Solution

A large-scale enterprise often owns branches or has partners. The branches and partners may connect via private lines or WANs to the headquarters of the enterprise. This networking mode is quite common for open enterprises but is also associated with severe security threats. To ensure that all the users accessing the intranet have a legal identity and conform to the security standards of the enterprise, EAD can be deployed on the routers at the branches and on the router or gateway in the enterprise headquarters so as to prevent user terminals accessing the network from causing security threats to the intranet.

VPN EAD Solution

Some enterprises and organizations allow their mobile office staff or partners to access the intranet via VPN. In the EAD solution, a VPN gateway is used to check the security status of a user terminal before the user terminal accesses the intranet and to apply enterprise security policies to the user terminal after the user passes the security authentication. If the intelligent client is not installed on the user terminal, the administrator can select to deny the user's access to the intranet or restrict the access rights of the user.

WLAN EAD Solution

An increasing number of external users and internal mobile subscribers start to access the enterprise network via WLAN cards. This, however, brings numerous security issues. The EAD system can interact with wireless equipment, such as FAT APs and ACs to authenticate the identity of users and check the security status of users before users can access and use the wireless network. Therefore, legal users can feel free to enjoy the convenience of the wireless network while facing less security threats from the air.

Gateway EAD Solution

In general, an enterprise will gradually recognize the necessity of security control of its internal network, especially the security of terminal users after the interconnection and interworking requirements are met. Then it is especially important to implement the secure access control of terminals. Usually the equipment of an enterprise network comes from multiple vendors. It is hard to use the equipment of only one vendor to exercise network admission control. In this case, one or multiple gateway devices can be used as the authentication controller and deployed in the core layer, in the data center, or at the network egress. The gateway devices use portal-based authentication and cooperate with the iNode client and the security policy server to implement EAD terminal admission control.

V. Networking Equipment Configuration

Mode	Description	Networking Restrictions	Requirements	
Monitoring mode	The administrator can monitor the security status of terminal users but cannot control and isolate users by technical means. The administrator can punish users (employees) by administrative means.	The access equipment is only required to support authentication. Dynamic ACL isolation is not required.	The access switch needs to support 802.1X.	
Alarm mode	The administrator can monitor the security status of terminal users and give alarm messages to users when users are online but cannot control and isolate users by technical means. The administrator can punish users (employees) by administrative means.	The access equipment is only required to support authentication. Dynamic ACL isolation is not required.		
Isolation mode	The administrator can monitor the security status of terminal users and can isolate users when users are online.	The access equipment is required to support authentication and dynamic ACL isolation.	802.1X authentication	H3C S3100EI, S3600SI/EI, S5100EI, S3610, S5510, S5600, S5500SI, S5500EI, S7500E
			Portal authentication	S5500EI, S7500E, S9500