H3C
ITоIP Solutions Expert

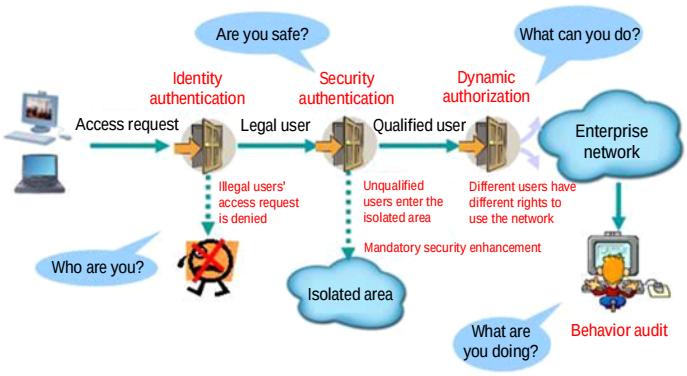
H3C EAD Access Control Solution

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.

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 effectively strengthen the active defense ability of user terminals, thus offering an effective and easy-to-use management tool for enterprise network administrators.

I. Overview

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.



II. Networking Model

The following figure shows the EAD 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.

III. Features

Comprehensive Admission Control

The EAD solution provides comprehensive access control and supports multiple access modes, including LAN access, WAN access, VPN access and wireless access. It can be deployed in numerous complex network topology modes (e.g. hub) and heterogeneous network environments (e.g. Cisco networks) to guarantee secure access of users in any mode from any place.

Strict Identity Authentication

In addition to identity authentication based on the user name and password, the EAD solution also supports the binding between user identities and the MAC addresses/IP addresses/VLANs of access terminals or the IP addresses and port numbers of access equipment. It supports smart card authentication and digital certificates, thus enhancing the security of identity authentication.

Complete Security Status Evaluation

Depending on the security policies configured by the administrator, users can check various items, including the virus database version of the terminal, terminal patches, application software installed on the terminal, whether any proxy server is installed on the terminal, dialup settings, assets management, software distribution, USB peripheral management, and remote assistance. To better meet customer requirements, the EA solution supports interaction with mainstream antivirus software vendors, such as Risen, Jiangmin, Kingsoft, Symantec, McAfee, Trend Micro, and Ahn. It can be used with industry desktop management products, including Microsoft SMS, LANDesk, and BigFix.

Integrating User Management and Network Device Management

- You can directly view user-related information in the access device list. As operations are simple and easy, the routine maintenance efficiency of the operator is improved.
- User operations can be performed on a selected access device, for example, you can forcibly disconnect all the users connected to a certain access device.
- You can click a certain access device in the online user list to directly view details about the access device of the current online user, such as the basic information, alarm information, and performance status of the access device. As operations are more user-friendly, the operator can gain better operation experience.

Integrating User Management and Network Topology Management

The topology map provides user management operations related to access devices and access terminals. For example, you can check user information, forcibly disconnect users, and perform security check. This makes terminal user management much more visual and clearer.

p

Role-Based Network Authorization

After a user terminal passes security information check (e.g. virus check and patch check), the EAD system can issue pre-configured access control policies to the security cooperation equipment or the client to normalize the network use behaviors of the user based on the user's role. The administrator can configure and implement security measures for terminal users, such as the user VLAN, ACL access policies, whether to forbid the proxy server, and whether to forbid dual network adapters.

Comprehensive ARP Attack Defense

In the EAD solution, the ARP gateway address is automatically issued and bound to ensure that terminal users are free from ARP spoofing attacks. In addition, the

EAD solution provides control measures such as ARP attack packet filtering and ARP abnormal traffic detection to prevent ARP attacks initiated by malicious users.

Desktop Assets Management

The EAD solution provides the comprehensive monitoring and management of terminal assets. The software and hardware use of user terminals can be monitored. In addition, the EAD solution supports the configuration management of terminal assets, the unified distribution of software, remote assistance, and desktop firewall management, thus helping customers more effectively manage their desktop assets.

USB Disk Audit and Peripheral Management

The EAD solution supports the monitoring of the access to USB disks and peripherals. You can check whether the USB disk is improperly used to copy important files. In addition, the EAD solution provides the management of USB disks and other peripherals. It can control the peripherals of terminal users so as to effectively prevent the disclosure of important information. This is still valid even when the peripherals are offline.

Eliminating the Need for the Client

The EAD solution provides simple deployment. Users need not install the client. Instead, the EAD system automatically loads the client to check the user identity and the security status of the user terminal. The user need not change its network access habits and can enjoy the security guarantee provided by the EAD solution.

Multi-Layer High Availability

The EAD solution provides 1+1 cold backup and 1+1 hot backup to prevent authentication service interruption that may occur upon failure of the EAD server when only a single EAD server is deployed. It also supports the emergency handling solution when a single device fails and allows the client to use the network without authentication in emergency cases, so as to guarantee the benefits of economy-sensitive users.

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. As H3C carries wide and deep cooperation with both Chinese and international antivirus software vendors, OS vendors, and desktop security product vendors, the EAD solution merges the merits of these vendors. The EAD system interacts with third-party authentication servers and security cooperation equipment via standard and open protocols. Therefore, the device interconnection and interworking is easy.

Flexible Deployment

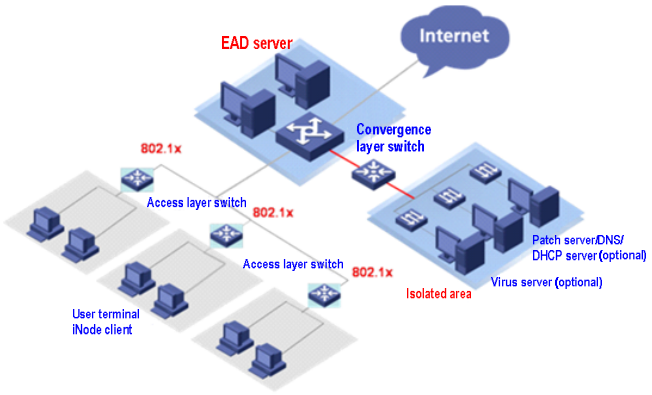
The EAD solution features flexible deployment and easy maintenance. The EAD system treats different users with different security policies configured by the network administrator. Different security check and processing modes, including the monitoring mode, the alert mode, the isolation mode, and the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

IV. Deployment

LAN EAD

User terminals usually access an intranet via a switch. The EAD solution 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 solution also forcibly implements security policies on users accessing the network so as to prevent security threats from the intranet.

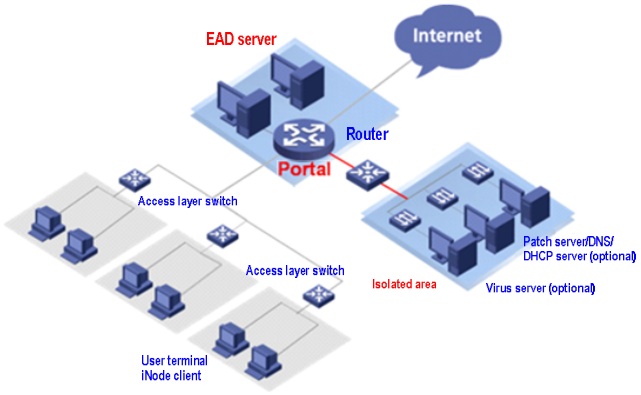
- 802.1x authentication in the access layer: strict control and high security.
- 802.1x authentication in the convergence layer: simple deployment and easy management. Hub users can be identified.



WAN EAD

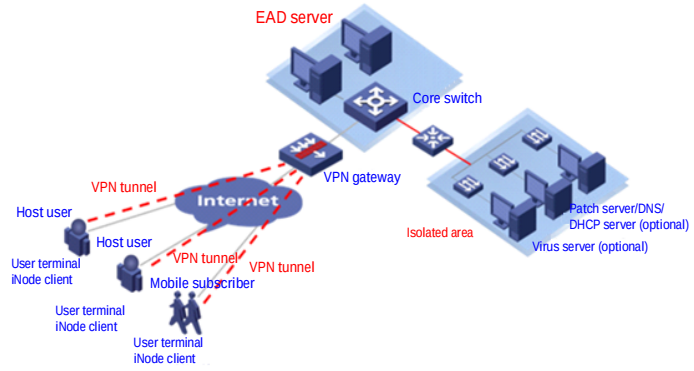
Enterprises that own branches or subsidiaries are often not strict in the management of branches and thus security vulnerabilities exist and the network may be out of control.

To address the above issues, H3C provides the WAN EAD solution. The backbone router or BRAS forcibly implements user portal authentication and checks the security status of user terminals, thus ensuring that only the users conforming to the standard security status requirements can access the headquarters network.



VPN EAD

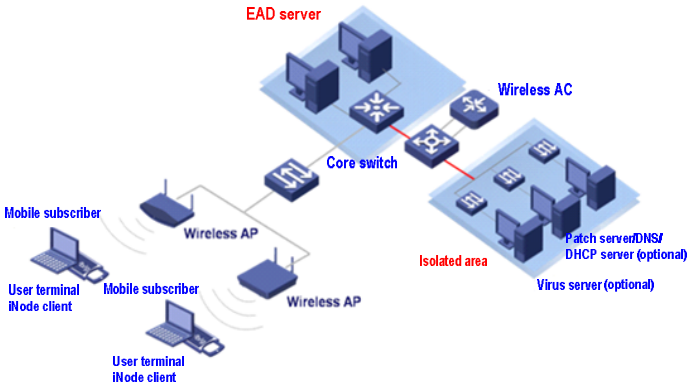
Some enterprises and organizations allow their mobile office staff or partners to access the intranet via VPN. In the EAD solution, a VPN gateway is used to check the security status of a user terminal before the user terminal accesses the intranet and to apply enterprise security policies to the user terminal after the user passes the security authentication. If the iNode 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

WLANs have incomparable merits than wired networks, e.g. easy installation, flexible use, cost saving, and easy expansion. For this reason, WLANs are more widely applied. This, however, also brings huge security threats to LANs.

In a wireless network, the EAD solution can be used to implement identity authentication, security check, and network authorization for wireless access users, thus effectively meeting the wireless access requirements of campus networks.



EAD for Heterogeneous Networks

In practical application, many user network environments often involve multiple vendors' equipment or even hubs. How can the EAD solution be deployed in such a heterogeneous network environment to provide terminal admission control, security check, user authorization, and behavior auditing? To address this issue, H3C launched an EAD gateway device. An EAD gateway can be connected via two links to the convergence layer equipment to implement portal-based user access control. In addition, an EAD server is deployed to implement admission policy control, security status check as well as identity authentication and security authentication.