H3C
ITоIP Solutions Expert

H3C ARP Attack Defense Solution

I. Preface

When a computer is normally connected but cannot open a web page or when the computer network is frequently disconnected and the Internet access speed is rather low, possibly ARP attacks exist in the network.

ARP attacks will cause network interconnection instability and users will not be able to access the Internet, or the enterprise network may be out of service and severe incidents may occur. Moreover, man-in-the-middle attacks may be further initiated by utilizing ARP attacks to illegally obtain the accounts and passwords of game, online banking and file service systems to cause huge loss to the victim. Therefore, ARP attacks are a kind of network attacks with severe consequences.

ARP attacks greatly threaten networks in all walks of life but no effective solutions are yet available. Even the well-known antivirus software and firewalls are helpless before ARP attacks. This is mainly because the Trojan Horse program used for ARP attacks usually disguises itself as a part of common software and is then downloaded and activated, or as a part of web pages and is then automatically transferred to the browser's computer and activated, or accesses the network through USB disks or mobile hard disks. Since the form and characteristics of the Trojan Horse program keep changing and updating, antivirus software usually does not work.

II. Overview

H3C launched effective ARP attack defense solutions according to the features of ARP attacks and actual market requirements.
H3C ARP Attack Defense Solution with Comprehensive Defense and Module Customization

H3C ARP attack defense solutions implement comprehensive defense from the top down through three control points: client, access switch, and gateway. Modules can be customized according to the specific network environment and customer requirements, thus offering diversified and flexible ARP attack defense solutions to users.

H3C provides two types of ARP attack defense solutions: monitoring mode and authentication mode. The monitoring mode is mainly applied to network environments where users dynamically access the network, whereas the authentication mode is mainly applied to network environments where users access the network after passing authentication. In practical deployment, a proper attack defense solution should be chosen according to the actual network scenario. In addition, the solution can be combined with H3C iMC to conveniently and visually configure gateway binding information and check the security status of users and equipment. This not only guarantees the overall security of the network, but also helps quickly discover insecure hosts and ARP attack sources in the network and enables quick response.

III. Solution Features

- Flexibility. H3C provides both the monitoring mode and the authentication mode. The networking is diversified and flexible.
- Comprehensive defense. Multiple modes can be combined to comprehensively defend against ARP attacks and practically guarantee the stability and security of the network.
- Investment protection. The solutions do not much rely on the access switch, and the existing equipment of the network can be well reused. Compatible with most of the existing network scenarios, the solutions effectively protect customers' investment.
- Adaptability. The solutions are adapted to dynamic address allocation and static address allocation and can be applied to various complex network environments by combining various modules such as terminals, access switches, and gateways.

H3C ARP attack defense solutions thoroughly solve the ARP

attack issue of customer networks, such as educational networks, financial networks, governmental networks, and enterprise networks. The “comprehensive defense and module customization” concept meets different requirements of old and new networks and emancipates users from ARP attacks!

IV. Typical Applications

u Unified Security Management

As there is no information exchange between different types of network and security devices, isolated information islands may easily occur. The SecCenter can manage network and security devices in a centralized way. It outputs analysis reports in real time after collecting, analyzing, correlating, summarizing, and uniformly processing bulky information, so as to help the administrator timely learn the security status of the existing network and help the administrator make analysis and decisions.

u Deep Integration of Security and Networks

H3C has accumulated rich technical experience in the network and security fields. Users can select to add the 10GE SecBlade firewall/IP module to the core switch. The 10GE SecBlade firewall/IP module provides complete security protection to meet the border isolation requirements of large-scale campus networks and internal areas, whereas no separate security equipment needs to be deployed. This simplifies the network structure, avoids single-point failures, facilitates management, and really implements the deep integration of security and networks.

u High Reliability

H3C equipment employs advanced technologies, such as 1+1 hot backup and L3 Monitor to implement 1+1 link backup and 1+1 gateway backup. When a link or a device fails, the system can timely discover the failure and perform automatic switching in a short time, thus greatly improving the network reliability and guaranteeing the uninterrupted running of user services.

u Virtual Security Service

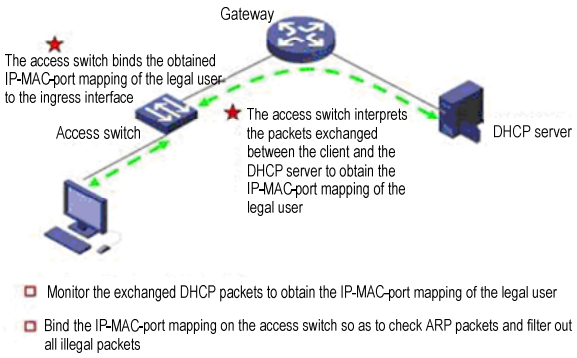
H3C SecPath firewall, UTM, and IPS products can provide the virtual security service. Multiple virtual systems are defined to separately deploy security policies for the multiple services of a user. When the user’s services change or a new service department is established, you can add or delete virtual systems to flexibly solve the subsequent network expansion requirements. This simplifies network management and effectively reduces the user’s security construction cost.

u Monitoring Mode

The access switch monitors the dynamic IP address allocation process of users so as to obtain and bind the IP-MAC mapping of the normal users. The access switch filters out all the ARP packets that do not match the bound IP-MAP mapping so as to prevent user hosts from initiating ARP attacks. This attack defense means can effectively guard against various ARP attacks. For some special clients such as printers and servers that adopt dynamic IP address allocation, entries can be manually added on the access switch to legally bind the IP-MAC mapping.

Figure 4-1 shows the service procedure.

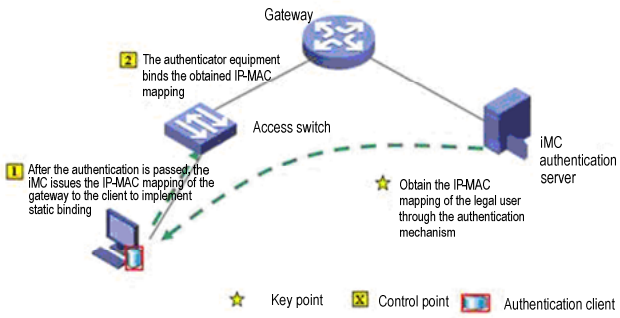
Figure 4-1 Monitoring mode



u Authentication Mode

As shown in Figure 2, an enhanced user authentication mechanism is employed to obtain the IP-MAP mapping of an access user and verify the legality of the user by means of authentication. The gateway IP-MAP mapping is pre-configured on the authentication server to manage the IP-MAP mapping information of the gateway in the network in a centralized way. When a legal user is online, the system filters out ARP packets or binds legal ARP information based on the above critical information, so as to effectively guard against ARP attacks. H3C defense solutions completely take into account the adaptability of solution implementation and can filter out ARP packets or bind legal ARP information according to the specific network environment. Figure 2 shows the service procedure.

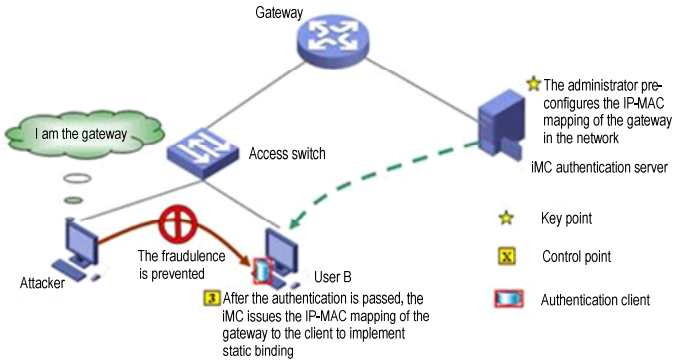
Figure 4-2 Authentication mode



Terminal Protection for the Authentication Mode

As shown in Figure 3, the iMC server issues the pre-configured gateway IP-MAC mapping to the iNode client during 802.1X user authentication. The iNode client searches all the network adapters on the user PC to find the matched gateway and implements static ARP binding of the IP-MAC mapping of the matched gateway on the PC, so as to effectively guard against ARP attacks to the gateway.

Figure 4-3 Terminal protection for the authentication mode



Access Binding for the Authentication Mode

As shown in Figure 4, extended 802.1X protocol packets are used during 802.1X user authentication. The EAPOL response packet (code =1, type = 2) carries the IP address of the user PC (the “Transfer IP address” option needs to be selected on the iNode client and it is recommended that the IP address and gateway be manually configured on the user PC). The access switch monitors the protocol packets during the 802.1X authentication process, binds the IP address, MAC address, and access port of the user PC to create an IP-MAC-Port mapping entry, and detects the ARP/IP packets from the user, so as to effectively prevent the user’s illegal ARP/IP packets from intruding the network. This is similar to the monitoring mode. For some special clients such as printers that cannot use the authentication means, the legal IP-MAC of the terminal may also be manually bound on the access switch

Figure 4-4 Access binding for the authentication mode.