An unsuccessful case of using security policy to block access to a domain name

Security 周天 2020-09-22 Published

Network Topology

Not involved

Problem Description

A local customer configures a domain name-based address object group and then blocks access to the address in security policy. The test failed.

Process Analysis

The test found that the address that the terminal accesses to the domain name resolved is different from the IP address that the domain name resolved on the firewall. If the security policy of the domain name is configured on the firewall, the firewall sends a DNS request to the DNS server to get the IP address of the domain name and save it.Then the security policy transforms the domain name-based policy into an IP address-based policy, followed by a common IP-based security policy match.That is, access control is achieved by releasing or blocking this IP address.When DNS table entries on the firewall age, the firewall re-initiates DNS queries, re-saves DNS table entries, and refreshes security policies.

The firewall did not block access to the domain name because the address resolved by the terminal accessing the domain name was different from the IP address resolved by the firewall.

If a domain name-based object group is configured, the DNS host table entry appears on the firewall immediately, which is the address that the firewall itself requests from the DNS server. The aging time is determined by the aging time (TTL) that the DNS response returned by the DNS server carries.

```
[H3C]display dns host
Type:
  D: Dynamic    S: Static

Total number: 1
No.  Host name            Type  TTL      Query type  IP addresses
1    www.sina.com.cn      D     44       A           115.238.190.238
```

For example, configuring security policies to prohibit access www.sina.com.cn, users are accessing www.sina.com.cn. When a DNS request is sent to the DNS server, the DNS resolved address (for example, 115.238.190.238) is obtained, and then the access to address 115.238.190.238 is blocked by the firewall.

Solution

It is recommended that both the intranet PC and the firewall have the same DNS server address. Otherwise, the same domain name may resolve out different addresses, affecting policy matching, or the intranet PC may point the DNS to the firewall, which acts as a DNS proxy.