Implementation of an IP access control technology

Information Technology
Issue 6, 2001

- 李蕾 (Li Lei)
- 乔佩利 (Qiao Peili)
- 陈训逊 (Chen Xunxun)

Keywords
IP access control; IP tunneling; OSPF; RIP; automata

Abstract

By utilizing technologies such as dynamic routing, IP tunneling, finite state automata, and packet capture, the dynamic blocking of harmful website IPs is achieved, together with source IP address statistics. The system is equipped with reliable validation mechanisms for activation and self-diagnostic capabilities.

0 Introduction

With the development of the INTERNET, effectively controlling network users' access to illegal websites has become a critically significant issue. For large ISPs with massive network traffic and multiple external egress routers, harmful IP addresses are blocked by manually configuring the egress routers via remote dial-in to their control ports. However, this approach would lead to two serious issues: (1) Dial-up configuration of the routers has to be done one by one through the control ports. Due to the large number of configuration entries and the low speed of router control ports, it would take more than ten minutes to complete a configuration and configuration check on a single router, which results in the unsynchronization across the controlled routers, and the high probability of error in manual operation and the instability of telephone dial-up lines further prolong the time for the configuration to take effect; (2) The configurations made through the router control ports must be saved to NVRAM, which has a limited number of rewrites. Frequent rewrites of NVRAM would cause damage to the system hardware, resulting in unimaginable consequences.

1 Design and implementation of the main functions of the system

By integrating IP tunneling and dynamic routing technologies, the following IP access control system is designed and implemented. The schematic diagram of the physical connection diagram of the system is illustrated in Figure 1.

The configuration host H0 and the configuration router R0 are directly connected through a 100BASE-Tx interface. R0 is connected to the campus network backbone via a 100BASE-Tx interface and establishes IP tunneling with the egress routers R1, R2, and R3 separately. Static routes and the RIP routing protocol are configured on H0, and the static routes are propagated to R0 via the RIP routing protocol. R0 and R1, R2, and R3 each enable the OSPF routing protocol, and add their respective IP tunneling virtual ports to the OSPF backbone area (area 0). The OSPF routing protocol on R0 is configured to enable it to learn the routing information from RIP and diffuse it to R1, R2, and R3. This logically forms a routing learning network based on the OSPF protocol. Since RIP is simple and supported by most server operating systems, and considering that there are only two nodes in the autonomous system formed between H0 and R0, RIP is used as the first-level routing learning protocol between H0 and R0. Between R0 and R1, R2, and R3, since they are connected through the backbone network, the RIP would introduce significant network overhead and is prone to causing broadcast storms which would negatively impact the communication within the larger network. Therefore, the link-state-based dynamic routing protocol OSPF is used as the routing learning protocol between R0 and the egress routers.

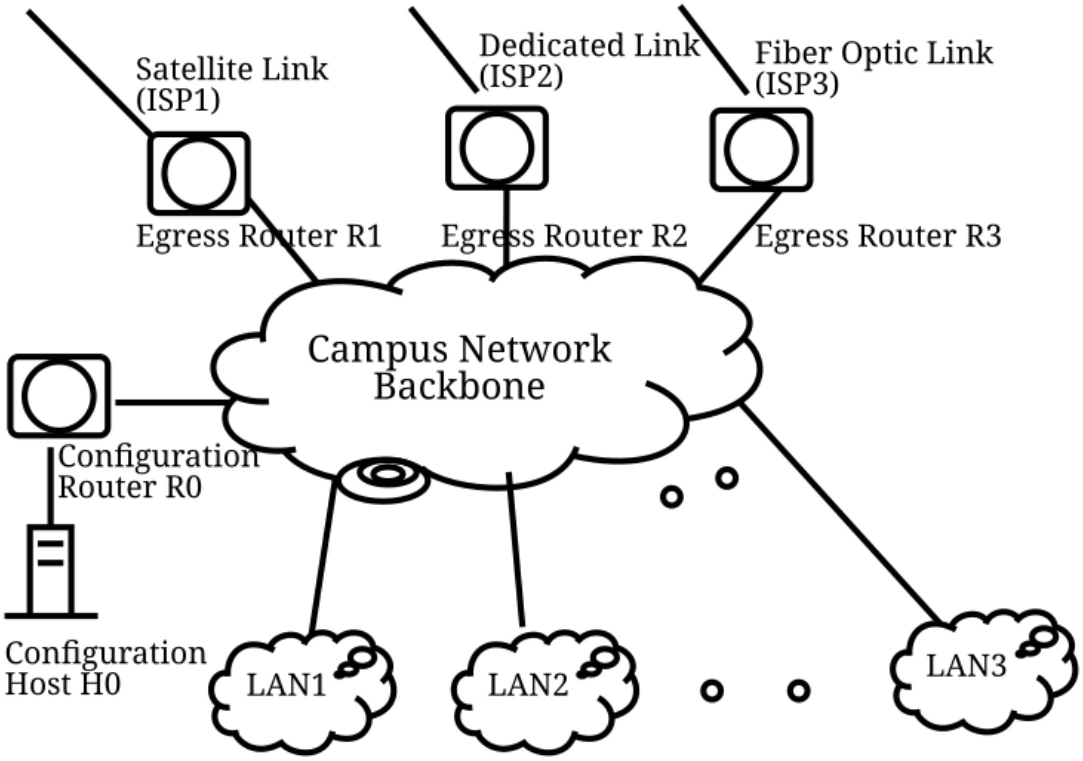

Figure 1: Schematic diagram of IP blocking system connection using dynamic routing learning method

Taking 204.177.92.196 as an example, bind the IP address on the network card fxp0 on host H0: `ifconfig fxp0 204.177.92.196 netmask 255.255.255.255`, and then perform a traceroute to 204.177.92.196 from one of the hosts H1 in LAN1. The result is as follows:

```
C:\>tracert -d 204.177.92.196
Tracing route to 204.177.92.196 over a maximum of 30 hops
1 <10ms <10ms <10ms R1 (IP address omitted)
2 <10ms <10ms  10ms R0 (IP address omitted)
2 <10ms <10ms  10ms H0 (IP address omitted)
Trace complete.
```

It can be seen that all packets accessing 204.177.92.196 have been routed to H0, which serves to block harmful sites. The advantages of using this blocking technology are as follows:

Efficiency: Since RIPv2 uses triggered updates for routing learning, the routing information will be broadcast to R0 as soon as the configuration of a harmful IP address on H0 takes effect, and the OSPF protocol on R0 learns the routing and then sends it to R1, R2, and R3 within a few seconds, so the efficiency is very high. Meanwhile, the order of magnitude of the synchronization time of the blocking routing information in R1, R2, and R3 is also on the order of seconds.

Security: Since the connection between H0 and R0 is point-to-point, there is no risk of IP spoofing. As the virtual internal network connection between R0 and R1, R2, and R3 is established using IP tunneling, with IP authentication and password authentication implemented at both ends of the tunnel, so it is safe and reliable.

Cost-effective: Only one additional configured router and one PC are required.

Wide applicability: Basically all routers support OSPF and RIP because the protocols used are RFC standard protocols.

Ease of use: All blocking operations for harmful IP addresses simply involve configuring an IP on the network card of H0.

2 Auxiliary functions of the system

In addition to the main functions described above, the system includes the following auxiliary functions. (1) Since dynamic routing protocols are used for blocking routing learning, it is difficult for network administrators to detect the impact on blocking routes in a timely manner when the link fails or the configuration of the egress routers is changed or a protocol failure occurs in large Internet organizations, so activation validation and protocol self-checking programs have been designed on H0. (2) In order to categorize and audit the IPs accessing harmful sites, IP packet capture is performed on H0 to summarize the statistics of all TCP request connection packets whose destination IPs are harmful addresses.

These two programs include activation validation and protocol self-checking, which perform checks on the blocking routing information on the egress routers and the operational status of the OSPF protocol. The Telnet client is written using finite state automata technology to accomplish automatic login to the egress routers and read the routing table configuration and OSPF protocol state, and multi-threading technology is used to allow simultaneous processing of multiple egress routers.

The TELNET unidirectional data stream is a typical intermittent character streaming data structure with control commands and data mixed in the same TCP stream, which is suitable for processing by means of a finite state machine. This module establishes a state machine for the TELNET protocol to implement the filtering of the TELNET data stream to filter out the control information (including TELNET command strings, ANSI control command strings, etc.) in the data stream. The following seven states are set:

STATE-TELNET-DATA	Master state, data state
STATE-TELNET-CMD	TELNET command state
STATE-TELNET-ANSI	ANSI command pre-filtering state
STATE-TELNET-ANSI1	ANSI command filtering state
STATE-TELNET-SUB1	Sub-negotiation filtering state
STATE-TELNET-SUB2	Sub-negotiation filtering pre-exit state
STATE-TELNET-WILLDO	OPTION negotiation filtering state

The state transition diagram is shown in Figure 2: (The content above the arrows is formatted as “Characters Received”/“Action Taken”.)

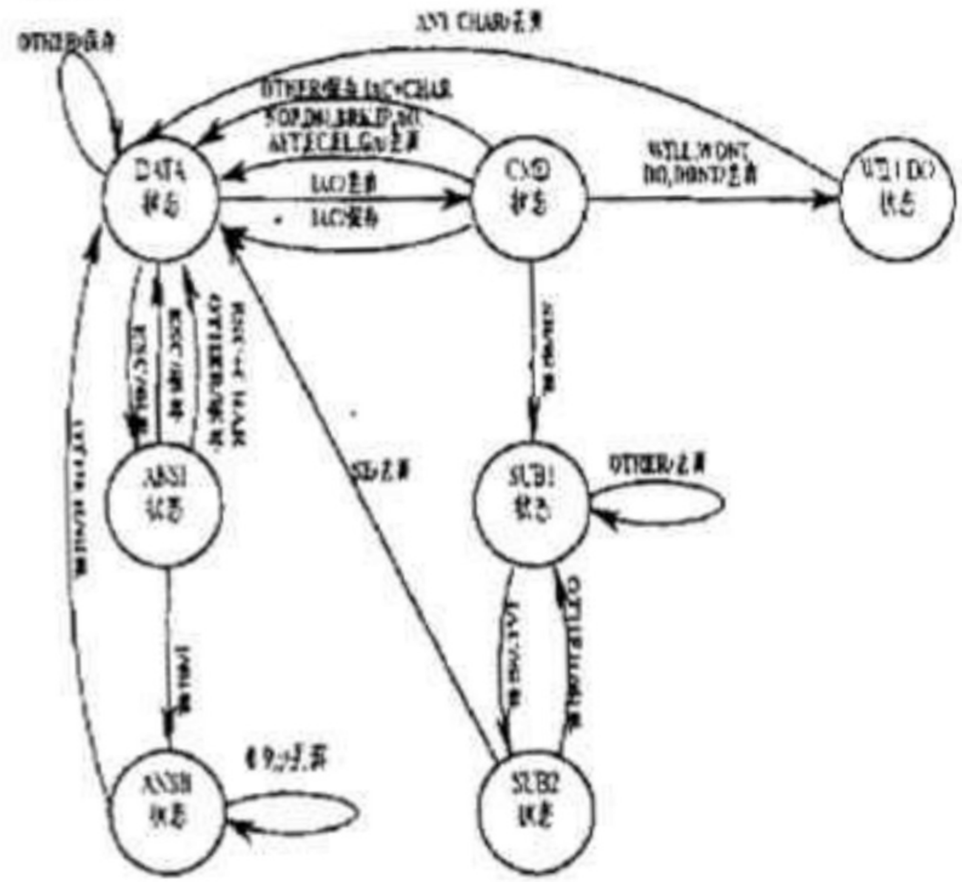

Figure 2: Telnet filtering state machine

Source IP classification statistics: This module consists of two programs: (1) Monitoring module, which uses packet capture technology to monitor the IP packets received on the network card of H0, and records in the log database the source and destination IP addresses of all TCP packets where the destination IP address is a harmful address and the SYN flag is set in the TCP header. The monitoring module is a background program (daemon) that works online in real time. (2) Statistical query module, which queries the logs generated by the monitoring module for statistics and generates a variety of non-classified statistical tables.

3 Conclusion

Dynamic routing and IP tunneling technologies are international standards with strong general applicability, making them suitable for deployment across Internet organizations nationwide. The finite state automata and packet capture technologies used are technologically advanced and highly efficient. After several months of practical operation, it has been demonstrated that the use of IP access control technology can efficiently, safely, and conveniently implement access control and auditing of harmful websites, delivering good practical results.

Author bios

李蕾 (Li Lei)
Harbin University of Science and Technology. Postal code: 150080
乔佩利 (Qiao Peili)
Harbin University of Science and Technology. Postal code: 150080
陈训逊 (Chen Xunxun)
Harbin University of Science and Technology. Postal code: 150080

[Date received: 2001-03-01 Editor in charge: 李光辉 (Li Guanghui)]