A Visual Approach for Modeling Firewall Configurations

Firewall is the most mature network security technology, but also the most common network security products in the market, in the Internet is a very effective network security tools. It is mainly to protect the information and structure of the internal network by shielding the outside world. It is set in the external and internal trusted network is not trusted network, the barrier between the can by means of the implementation of security policy to control the information more widely into the trusted network, prevent unexpected potential invasion damage, it can also limit the trusted network users in the unauthorized access to external network, thus weakened the function of the network.

1) Filtering firewall

Filtering firewall is in the network layer and transmission layer, can be based on the address of the data source and protocol type and other identifying characteristics of analysis, to determine whether it can be passed.

Implement:

The firewall directly obtains the packet's IP source address, destination address, TCP/UDP source port, and TCP/UDP destination port.

(2) Application of proxy type firewall

The application proxy firewall works primarily at the highest OSI layer, above the application layer. Its main feature is that it can completely isolate the network communication flow, and the application layer can be supervised and controlled by a specific agent.

Implement:

The firewall ACTS as an intermediate node for access, a firewall for the client is a server, and a firewall for the server is a client.

(3) State detection firewall

State detection firewall is a kind of advanced communication filtering. It examines application layer protocol information and supervises the status of connection-based application layer protocols.

Implement:

State detection firewalls dynamically determine whether messages can pass through firewalls by detecting the connection status of several TCP/UDP connections.

CHEN ZIMING

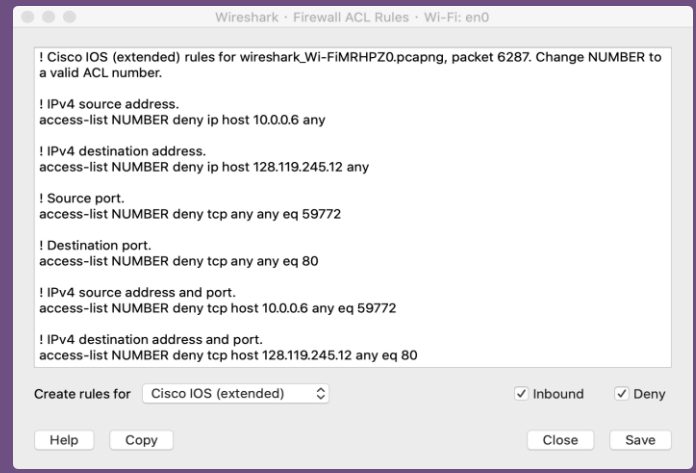
zmc19jdc@bangor.ac.uk

Supervisor:

Saad Mansoor

METHOD:

WIRESHARK is the world's foremost and widely-used network protocol analyzer. It lets you see what's happening on your network at a microscopic level and is the de facto (and often de jure) standard across many commercial and non-profit enterprises, government agencies, and educational institutions.



Technology:

1. Packet filtering technology

The packet filtering technology of the firewall is generally only applied to the data of the model network layer of OSI7 layer, which can complete the state detection of the firewall, thus the logical strategy can be determined in advance.

2.Encryption technology

relevant personnel can effective encrypted transmission of information, including information master password are on both sides of communication, to accept the information people need to decrypt the encrypted data processing, to obtain the data transmission of information, the firewall encryption technology applications, are aware of information encryption processing safety guarantee.

3. Anti-virus technology

it mainly includes the prevention, cleaning and detection of viruses and other aspects.