Host Firewalls and Antivirus Software

www.huawei.com

Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

Foreword

- Firewalls were first applied to buildings to isolate fire and prevent fire from spreading from one area to another.
- In the communications field, firewalls are mainly used to protect a network against attacks and intrusions from other networks.
- Antivirus software is a type of program tool that is used to remove known harmful program code, such as viruses and Trojan horses, from computers.

Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.

Objectives

- Upon completion of this course, you will be able to:
  - Describe the definition and categories of firewalls.
  - Describe the main functions of firewalls.
  - Describe the concept of antivirus software.
  - Distinguish antivirus software from firewalls.

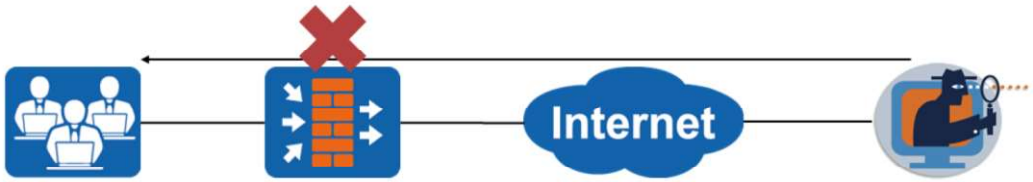
Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.

Contents

Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.

What Is a Firewall?

- A firewall is a method of separating private networks from public networks (such as the Internet). It is actually an isolation technology. A firewall allows only authorized people and data to access a network and prevents access from hackers. If data fails to pass through a firewall, people on an intranet cannot access the Internet, and people on the Internet cannot communicate with people on the intranet.



Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.

- The firewall technology is a specific security technology. The term "firewall" was originally used to describe the wall built between buildings to prevent fire from spreading.
- Firewall = Hardware + Software + Control policies
- Control policies:
  - Permit unless otherwise specified
  - Deny unless otherwise specified

Firewall Classification

- By form:
  - Hardware firewalls
  - Software firewalls
- By protected object:
  - Standalone firewalls
  - Network firewalls

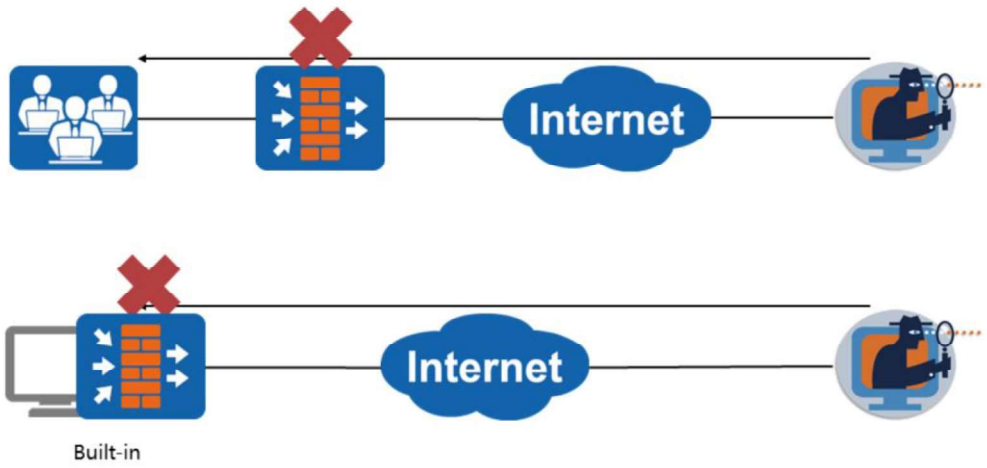
Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Hardware firewall: uses an embedded system, which is generally open-source. Hardware firewalls are used to isolate internal and external networks through a combination of hardware and software.
- Software firewall: is generally installed on an OS platform. A software firewall isolates internal and external networks by means of software.
- Standalone firewall: serves only the current host.
- Network firewall: serves a specific network.

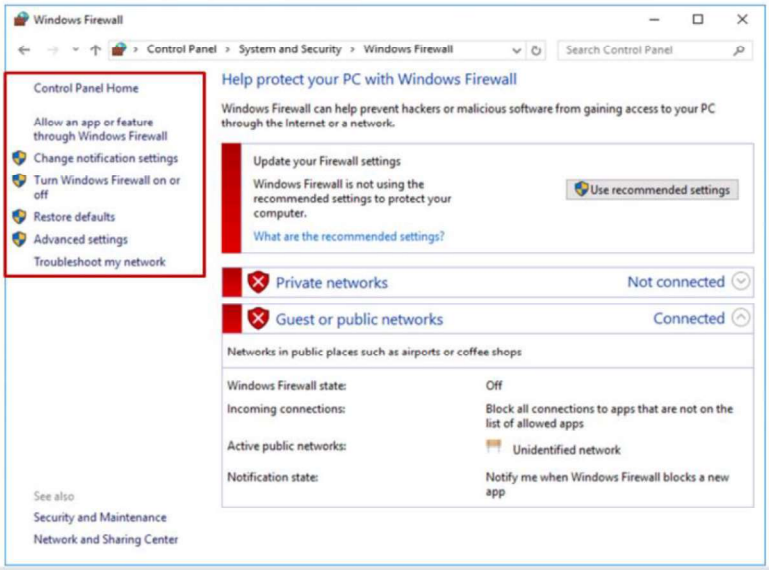
Windows Firewalls

- A Windows firewall is a software firewall built in the Windows OS.



Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.

Windows Firewall Settings



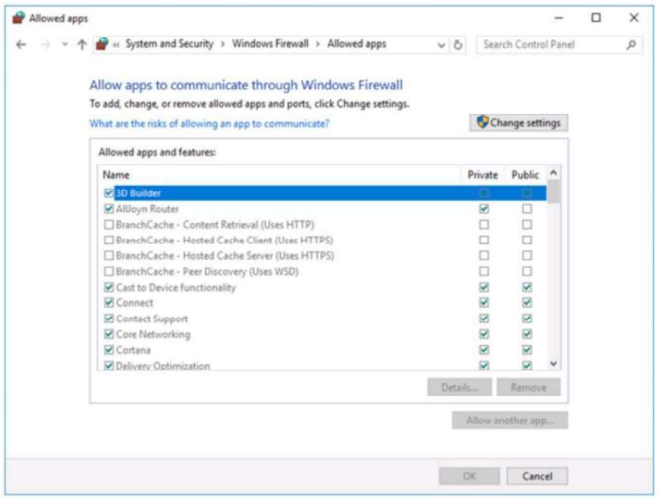
Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Allow an app or feature through Windows Firewall: specifies a data pass-through rule.
- Change notification settings: specifies a notification rule.
- Turn Windows Firewall on or off: enables or disables the Windows firewall.
- Advanced settings: specifies detailed inbound & outbound rules and connection security rules.
- Restore defaults: restores the Windows firewall to its default settings.
- Troubleshoot my network: detects network issues.

Windows Firewall Rule Settings

- Allow an app or feature through the Windows firewall.



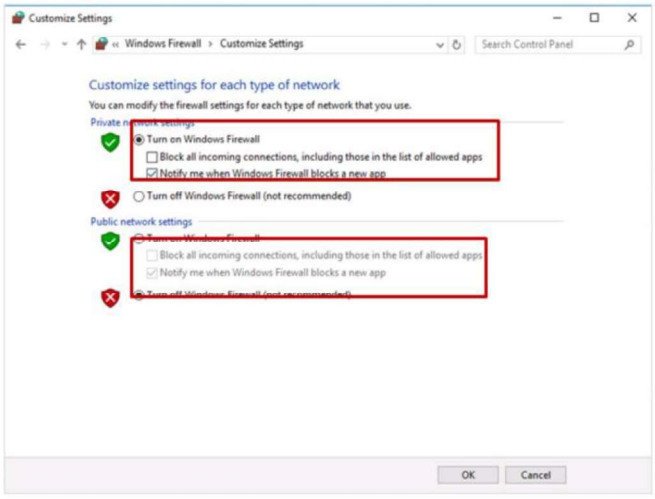
Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Change settings: adds, changes, or removes allowed apps and ports.
- Details: displays the details of allowed apps and features.
- Remove: removes apps or features from Allowed apps and features.
- Allow another app: adds an app or feature to Allowed apps and features.
- You can select apps and features from Allowed apps and features and apply them to a home/work (dedicated) network or a public network.

Windows Firewall Notification Rule

- Modify a notification rule.

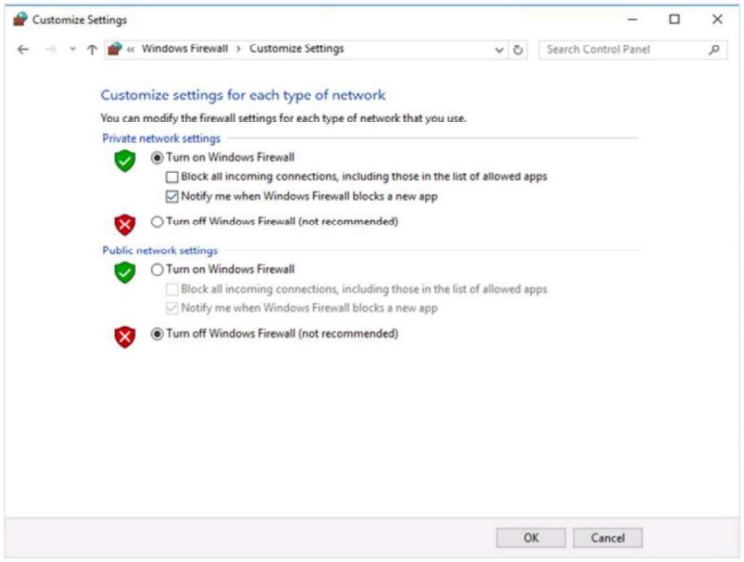


Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- When a Windows firewall is enabled, you can determine whether to send a notification when the firewall blocks new apps.

Enabling or Disabling a Windows Firewall



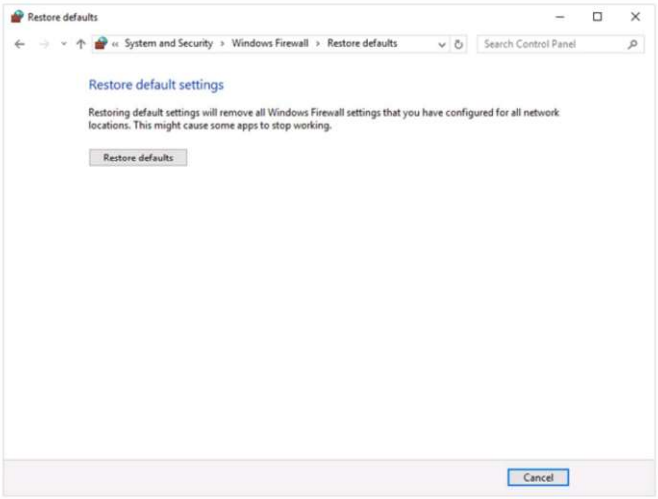
Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Enable the firewall for a type of network for security protection, or disable the firewall so that all apps can pass through.
- The window for enabling or disabling change notification is the same as that for enabling or disabling the Windows firewall.

Initializing Windows Firewall Settings

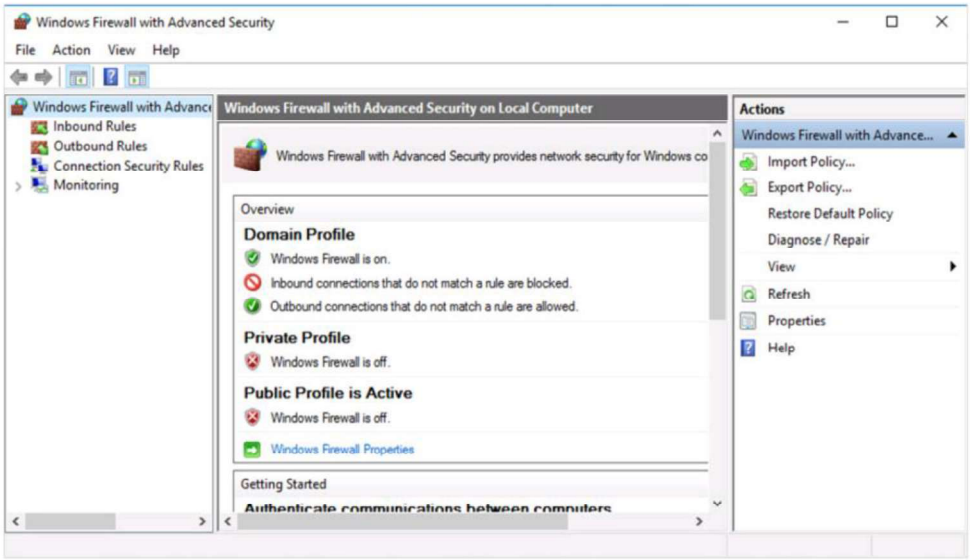
- Restore default settings.



Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.

- If firewall rules are not set properly, malicious network attacks may not be blocked, and users may fail to access the Internet. If such a situation occurs, click Restore defaults to restore the Windows firewall to the default settings.

Advanced Windows Firewall Settings

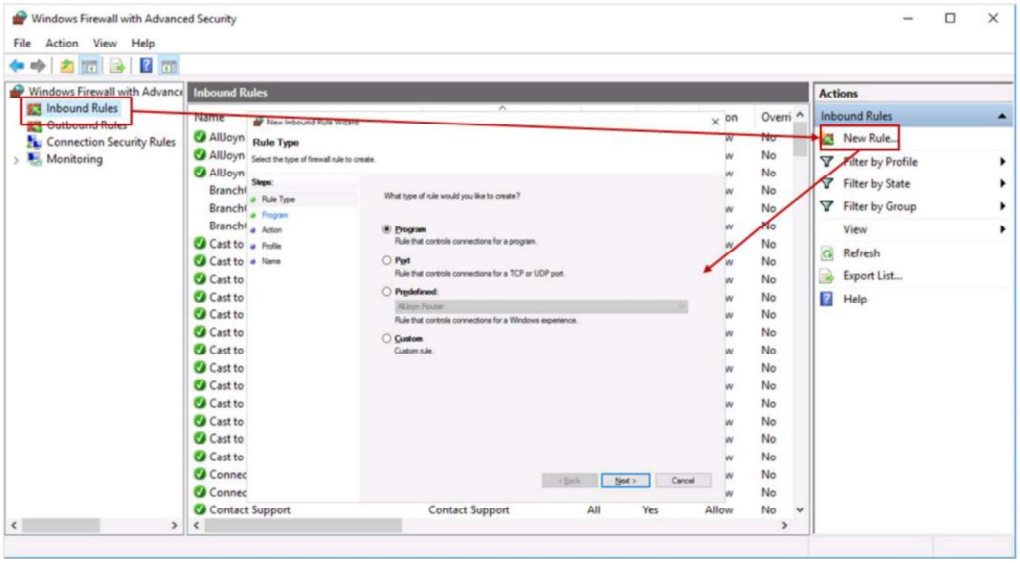


Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- If settings of Allow an app or feature to through Windows Firewall cannot meet your requirements, you can access the Windows Firewall with Advanced Security window to set more detailed rules.
- Settings in this window allow you to customize inbound rules, outbound rules, and connection security rules, and monitor the firewall.

Windows Firewall Rule Settings



Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Program: specifies a rule that controls connections for specific local programs or all programs when they use public (or home) networks.
- Port: specifies a rule that controls connections for specific local ports or all ports when they use public (or home) networks.
- Predefined: specifies a predefined rule that controls connections.
- Custom: specifies a rule that controls connections for specific local programs when they use public (or home) networks through predetermined source and destination ports and IP addresses.

Contents

Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.

Iptables Introduction

- Iptables is a free packet filtering firewall. It evolves along with the development of the Linux kernel, and has undergone four phases:
  - 1.1 kernel: ipfirewall
  - 2.0 kernel: ipfwadm
  - 2.2 kernel: ipchains
  - 2.4 kernel: iptables

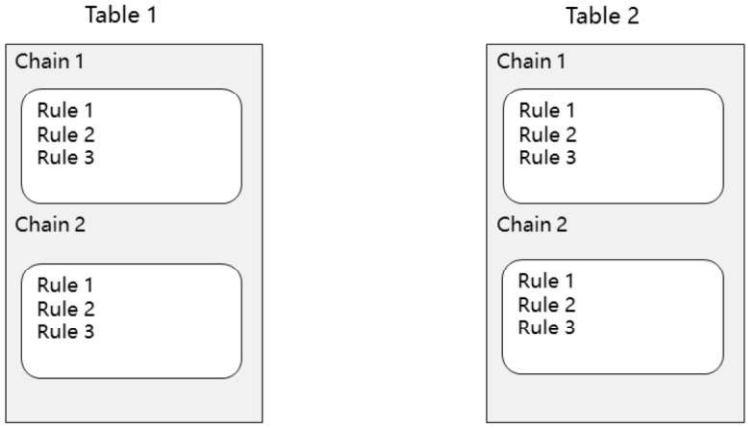
Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- A Linux firewall consists of two components: netfilter and iptables. Iptables is an interface between a firewall and users, while netfilter provides firewall functions.
- netfilter is a framework in the Linux kernel. It provides a series of tables. Each table consists of several chains, and each chain consists of several rules.
- Iptables is a user-level tool which can add, delete, and insert rules. These rules tell the netfilter component how to process data packets.

Iptables Structure

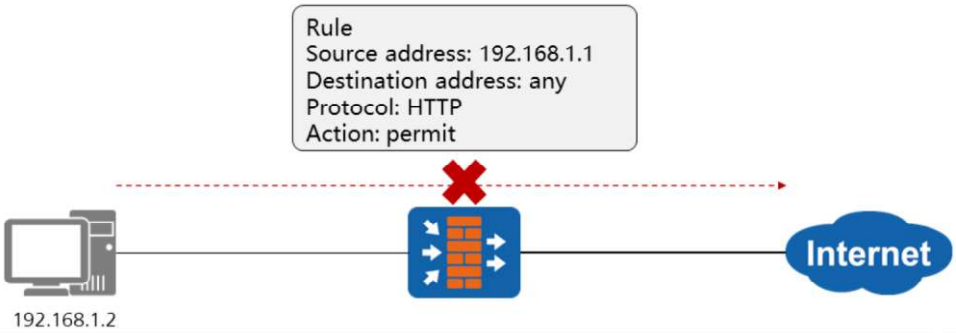
- Iptables structure: iptables > table > chain > rule. A table consists of chains, and a chain consists of rules, as shown in the following figure.



Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.

Basic Concepts of Iptables - Rule

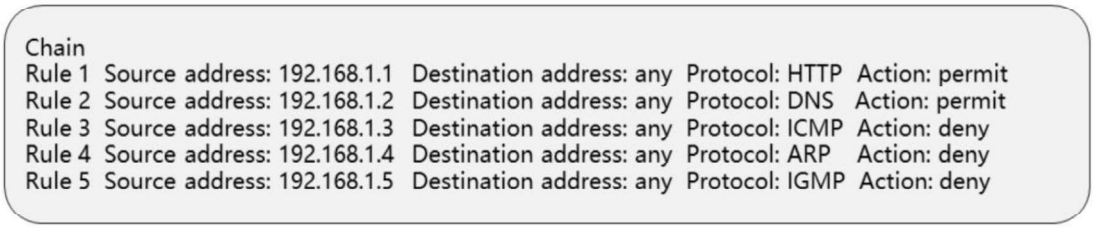
- If a data packet matches a rule, the packet is processed according to the rule.
- An iptables rule specifies quintuple information including the source address, destination address, source port, destination port, and protocol.
- If a data packet matches an iptables rule, iptables processes the packet according to the method defined in the rule, for example, allowing the packet to pass through or discarding the packet.



Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.

Basic Concepts of Iptables - Chain

- A chain is a path for transmitting data packets. Each chain contains one or more rules. When a data packet reaches a chain, iptables matches the packet with the first rule in the chain and checks whether the packet meets the conditions defined in the rule.
- If yes, iptables processes the packet according to the action defined in the rule. If no, iptables matches the packet with the next rule.
- If the packet does not match any rule in the chain, the default policy in the chain is used.



Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Iptables contains five rule chains:
  - PREROUTING
  - INPUT
  - FORWARD
  - OUTPUT
  - POSTROUTING
- These are the five rule chains defined by netfilter. Any data packet passing through will reach one of these chains.

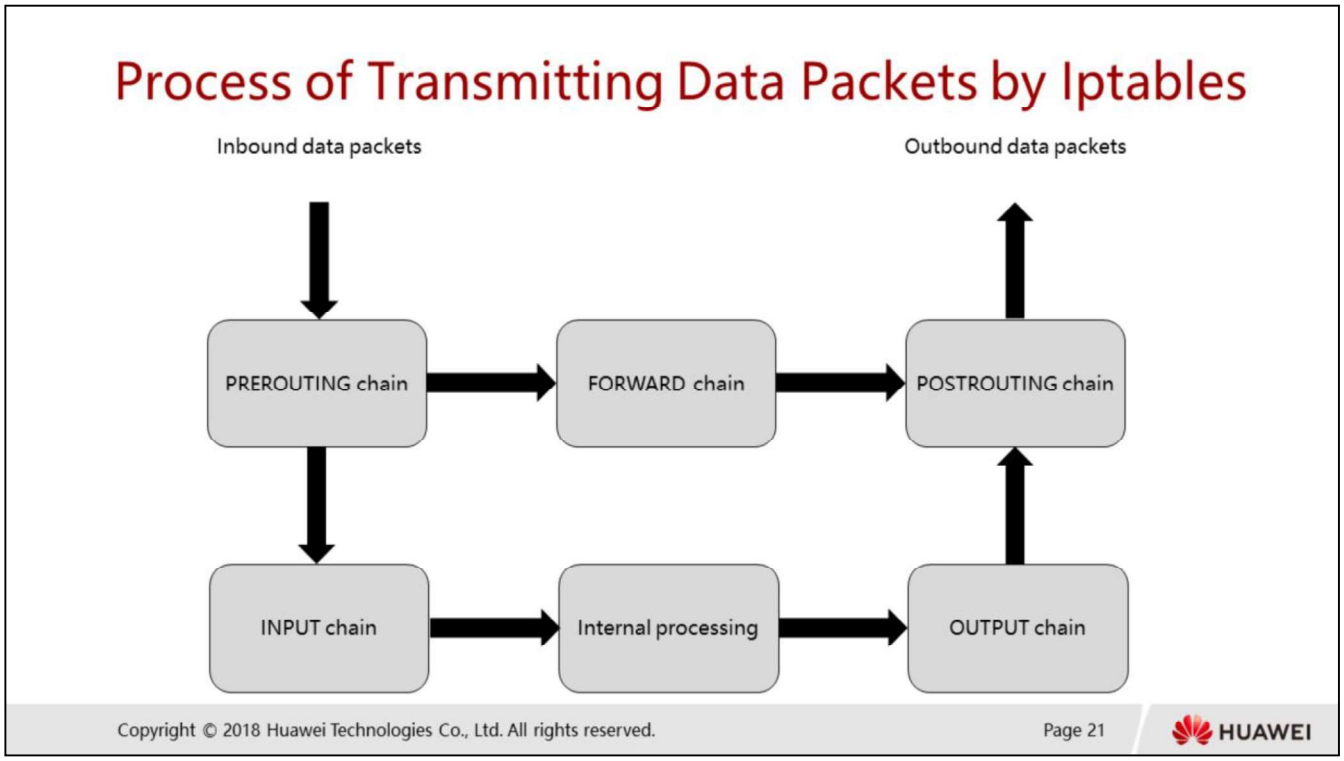
Basic Concepts of Iptables - Table

- Tables provide specific functions. Iptables contains four tables:
  - filter table: permits or denies data packets.
  - nat table: translates addresses.
  - mangle table: modifies packet data.
  - raw table: determines whether data packets are processed using the state tracking mechanism.
- Table priority: raw > mangle > nat > filter.

Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Generally, three chains are allowed in a filter table: INPUT, FORWARD, and OUTPUT.
- Generally, three chains are allowed in a nat table: PREROUTING, OUTPUT, and POSTROUTING.
- All the five chains are allowed in a mangle table: PREROUTING, INPUT, FORWARD, OUTPUT, and POSTROUTING.



- When a data packet enters a network adapter, it is first matched with the PREROUTING chain. The system determines the subsequent processing according to the destination address of the packet. Possible processing:
  - If the destination address of the packet is the local host, the system sends the packet to the INPUT chain to match the packet with rules in this chain. If the packet matches a rule, the system sends the packet to the corresponding local process. If no match is found, the system discards the packet.
  - If the destination address of the packet is not the local host, the packet will be forwarded. The system directly sends the packet to the FORWARD chain to match the packet with rules in this chain. If the packet matches a rule, the system sends the packet to the corresponding local process. If no match is found, the system discards the packet.
  - If the packet is locally generated, the system directly sends the packet to the OUTPUT chain to match the packet with rules in this chain. If the packet matches a rule, the system sends the packet to the corresponding local process. If no match is found, the system discards the packet.

Iptables Rules

- Iptables rules are complex.
- Format: iptables [-t table] COMMAND chain CRITERIA -j ACTION
  - -t table: specifies the table to which the rule applies. It can be filter, nat, mangle, or raw.
  - COMMAND: defines how to manage rules.
  - chain: specifies a chain, and can be omitted when you define a policy.
  - CRITERIA: specifies matching criteria.
  - -j ACTION: specifies the action to be taken.
- For example, access to 172.16.0.0/16 is not allowed.
  - iptables -t filter -A INPUT -s 172.16.0.0/16 -p udp --dport 53 -j DROP

Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.

Contents

Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.

What Is Antivirus Software?

- Antivirus software is a type of software used to remove computer viruses, malicious software, Trojan horses, and other computer threats.
- Antivirus software provides functions such as monitoring, identification, virus scanning, virus clearing, automatic upgrade, and proactive defense.

Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.

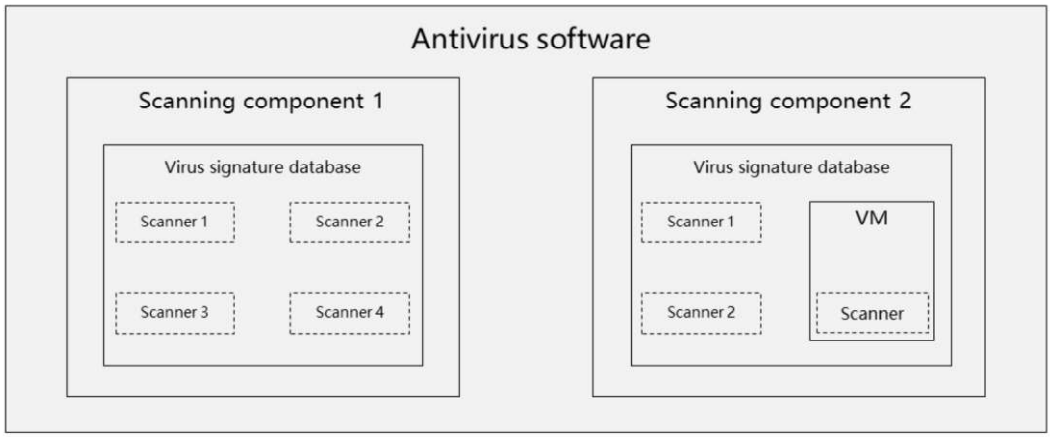
Basic Functions of Antivirus Software

- Virus prevention: prevents viruses from attacking computers.
- Virus identification: scans for viruses in the programs or files running on a computer and compares the viruses against the virus signature database to identify them.
- Virus clearing: restores infected objects according to different types of viruses and their infection characteristics.

Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.

Antivirus Software Components

- Antivirus software consists of scanners, a virus signature database, and a VM, which are integrated by a main program.



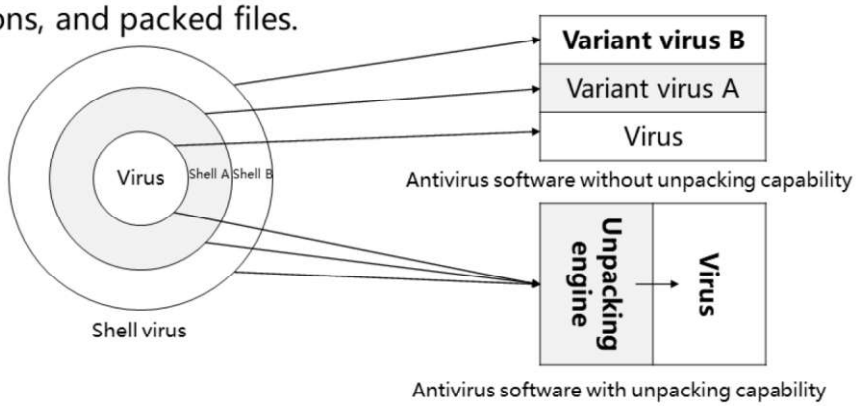
Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Scanners are the main part of antivirus software and are mainly used to scan viruses. The antivirus effect of antivirus software depends on how advanced the scanner compilation technology and algorithm are. Therefore, most antivirus software has more than one scanner.
- The virus signature database stores virus signatures, which are classified into memory signatures and file signatures. Generally, file signatures exist in files that are not executed. Memory signatures generally exist in a running application program.
- A VM enables viruses to be run in a virtual environment built by antivirus software.

Key Technologies of Antivirus Software - Unpacking

- The unpacking technology is commonly used by antivirus software. This technology can be used to analyze compressed files, files with misleading instructions, and packed files.

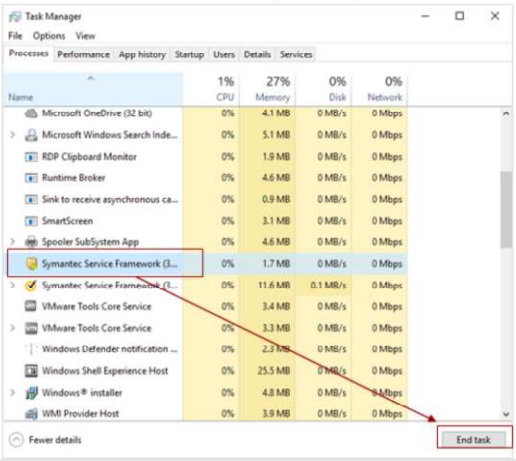


Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.

- If antivirus software does not have a strong unpacking capability, two different signature records must be added to defend against shell viruses. This is because if a hacker uses another tool to pack a virus, the virus will not be recognized by the antivirus software, and a new signature record must be added for removing the virus.
- If antivirus software has a strong unpacking capability, it unpacks the virus file, and then scans and kills the virus. In this way, only one signature record is enough. This reduces the occupation of system resources by the antivirus software, and greatly improves the antivirus software's capability to scan and kill viruses.

Key Technologies of Antivirus Software - Self-protection

- The self-protection technology prevents viruses from ending the running process of antivirus software or tampering with antivirus software files.



Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.

Key Technologies of Antivirus Software - Repair

- Antivirus software usually deletes infected files to remove viruses. In this case, some system files may be deleted by mistake. As a result, the system breaks down and cannot start. The repair technology of antivirus software repairs damaged files.

Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.

Key Technologies of Antivirus Software - Real-Time Update

- The virus signature database of antivirus software is usually lagged behind computer viruses. Therefore, the real-time update of the virus signature database is particularly important.

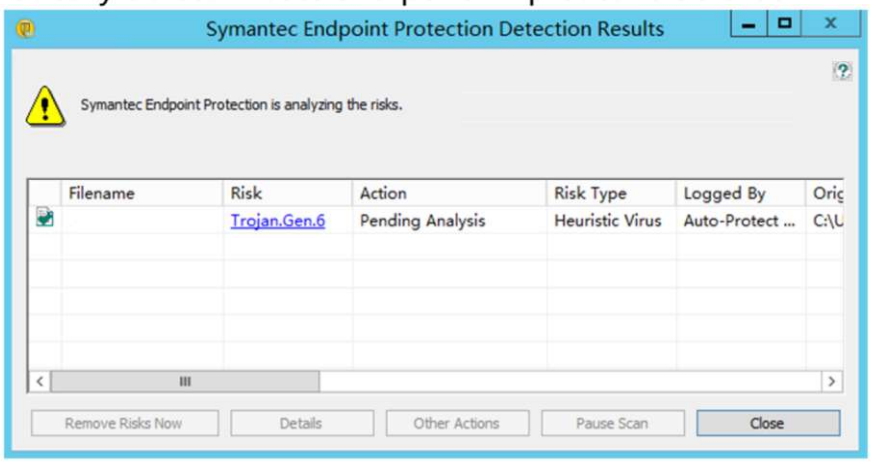
Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Currently, a more advanced cloud antivirus technology can be used to access the virus signature database on the cloud in real time. Users do not need to update their local virus signature database frequently.

Key Technologies of Antivirus Software - Proactive Defense

- Antivirus software can also monitor program actions and files to automatically detect viruses and perform proactive defense.

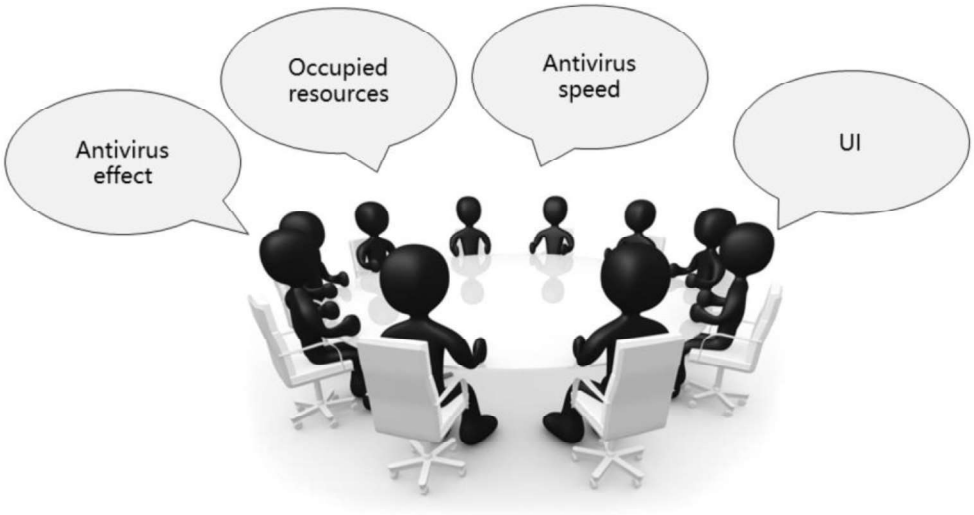


Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.

Mainstream Antivirus Software in China

Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.

What Antivirus Software Do Users Need?



Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.

Common Knowledge of Antivirus Software

- Antivirus software cannot scan or kill all viruses.
- Antivirus software cannot kill all scanned viruses.
- It is unnecessary to install two or more sets of antivirus software on one OS of a computer (unless for compatible or green versions), although many types of antivirus software are compatible. In addition, you are advised to view the list of incompatible programs.
- Antivirus software may clear, delete, forbid access to, or isolate infected files. It also may not process the files.

Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Clear: Clear worms from infected files to restore the files.
- Delete: Delete virus files. These files are not infected but contain viruses. They cannot be cleared.
- Forbid access: Do not access virus files. After a virus file is detected, if you choose not to process the file, the antivirus software may deny access to this file. When you attempt to open such a file, an error message "not a valid win32 application" is displayed.
- Isolate: After a virus file is deleted, the file is moved to the isolation area. You can retrieve deleted files from the isolation area. Files in the isolation area cannot run.
- No process: If you are not sure whether a file contains viruses, do not process it temporarily.
- Most antivirus software is lagged behind computer viruses. In addition to updating antivirus software in a timely manner and periodically scanning your computer: update your computer and network security knowledge, do not open unknown files or insecure web pages, update your password as required, and use the security assistant and personal firewall. These measures will better protect your computer and network security.

Quiz

1. Which of the following categories does a Windows firewall belong?
   A. Hardware firewalls
   B. Software firewalls
   C. Standalone firewalls
   D. Network firewalls
2. Which of the following are components of antivirus software?
   A. Scanner
   B. Virus signature database
   C. VM
   D. Firewall

Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.

HUAWEI

- Answers:
  - BC
  - ABC

Summary

- Firewall Overview
- Antivirus Software

Copyright © 2018 Huawei Technologies Co., Ltd. All rights reserved.

Thank You

www.huawei.com