

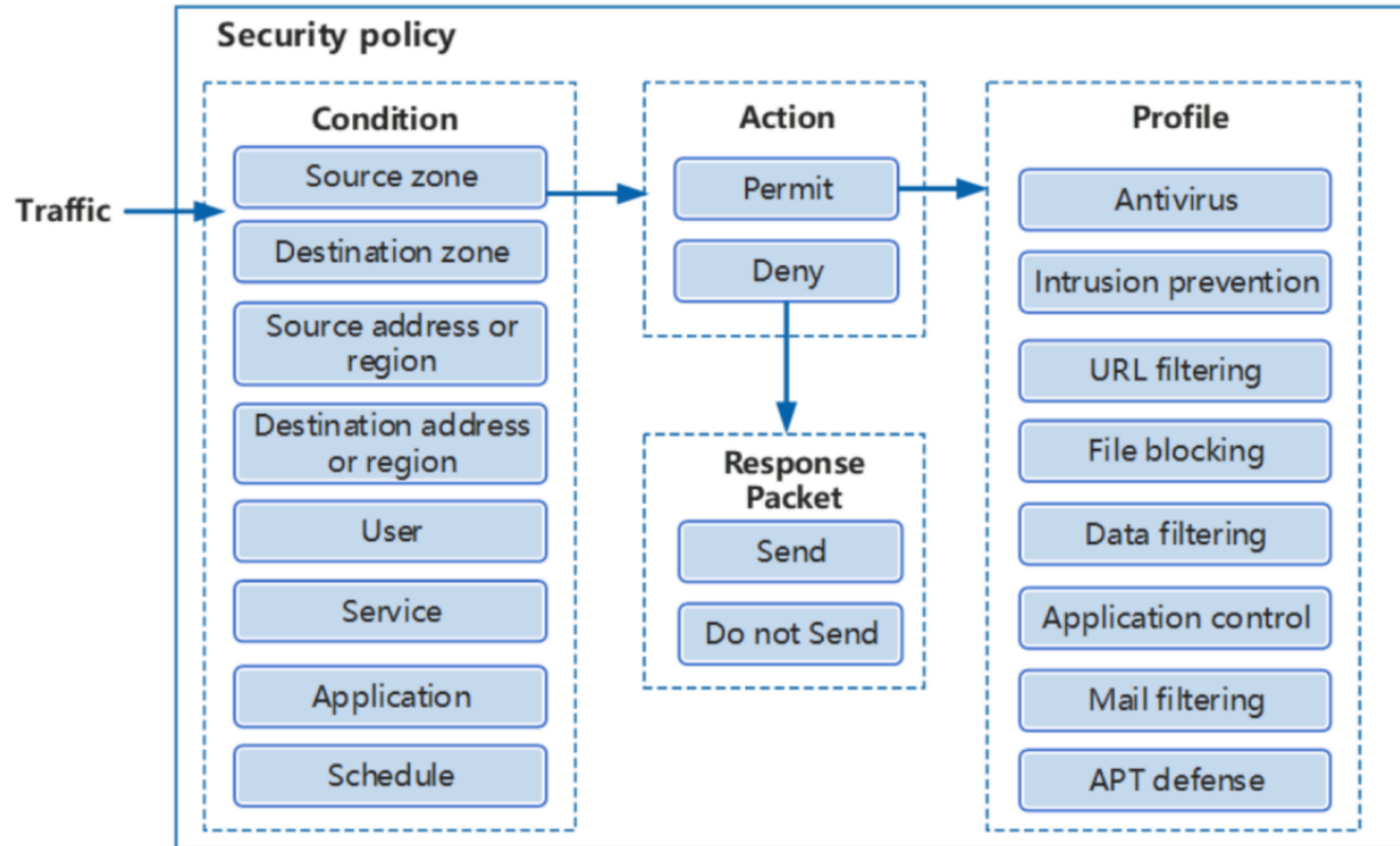
Firewall Security Policies and Application

Lecture 6

HCIA-Security

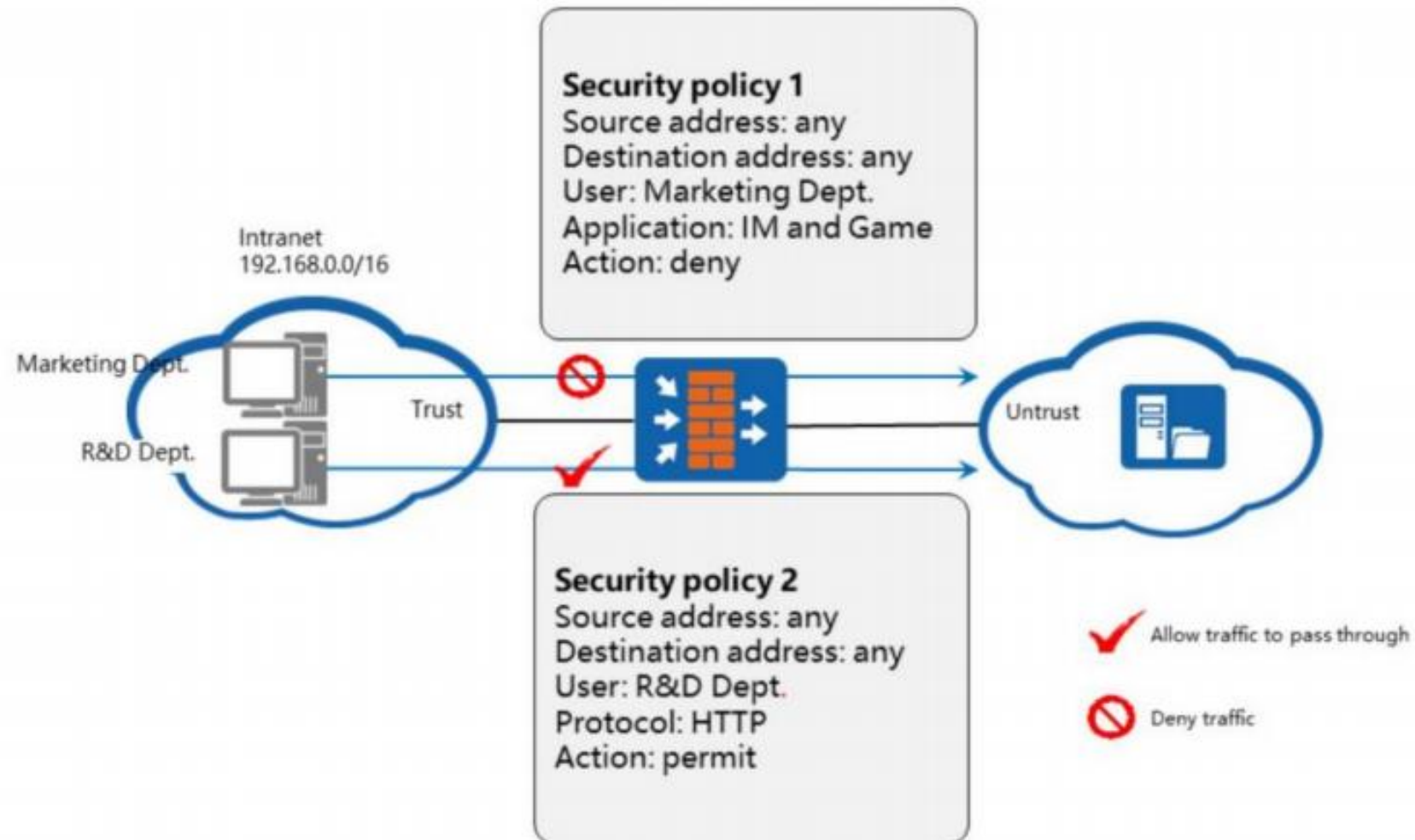
Prepared by
Dr. Abdelrhman Ahmed

Security Policy Matching Process



Chapter
06

Application of Security Policies



Application of Security Policies

- Compared with conventional security policies, the security policies on NGFWs can:
 - Distinguish between employees from different departments based on "users" , making network management more flexible and visualized.
 - Distinguish between applications (such as web IM and web game) using the same protocol (such as HTTP), achieving refined network management.
 - Inspect content security and block viruses and hacker intrusions to better protect internal networks.

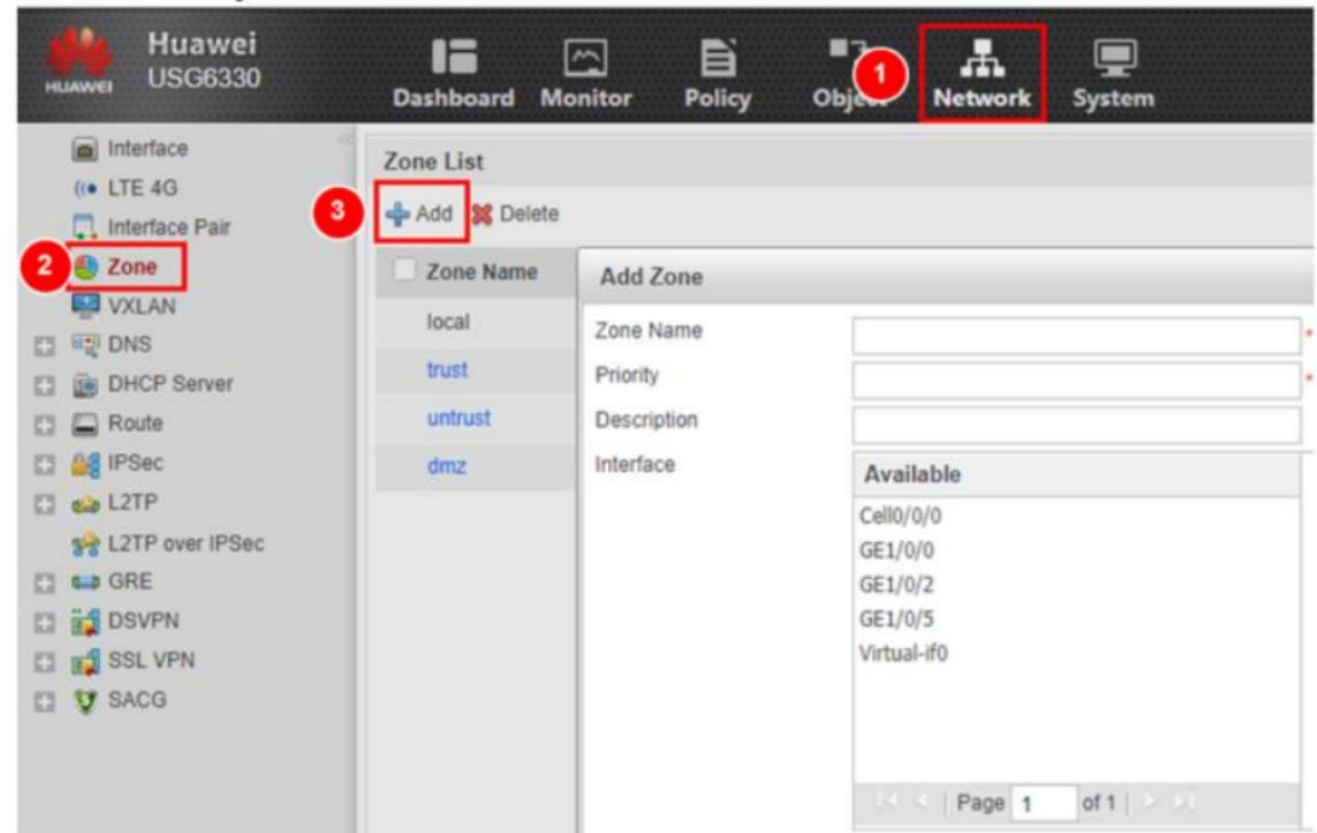
Chapter
06

Configuring a Security Zone on the Web UI

- The system has four default security zones. If more security levels are needed, you can create a security zone and define its security level.

- Procedure for creating a security zone:

- ☐ Choose Network > Zone.
- ☐ Click Add.
- ☐ Set security zone parameters.



Chapter
06

Configuring a Security Policy on the Web UI

- A security policy includes:

- Matching conditions: Source security zone, destination security zone, source address, destination address, user, service, application, and schedule
- Action: Permit or deny
- Content security profile (optional): Antivirus, intrusion prevention, URL filtering, file blocking, data filtering, application behavior control, mail filtering, and APT defense

- The firewall can identify traffic attributes and match the attributes with security policy conditions. If all conditions of a security policy are matched, the traffic matches the security policy. The firewall takes the action defined in the matched security policy on the traffic.

- If the action is permit, the firewall inspects the traffic content. If the traffic passes the content security inspection, the traffic is allowed to pass through. If not, the traffic is denied.

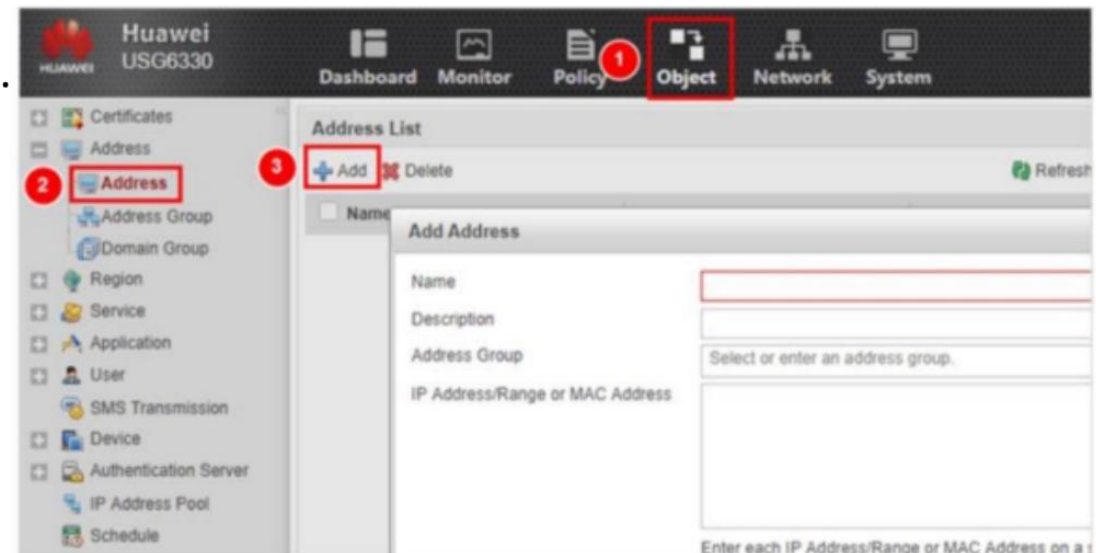
- If the action is deny, the traffic is denied.

Security Policy List																
+ Add Security Policy + Add Security Policy Group ✖ Delete 📄 Copy ↕ Move 📄 Insert 📄 Export 🔄 Reset All Statistics 🟢 Enable 🔴 Disable 🛠 Customize 📄 Expand 📄 Collapse 🔄 Refresh Enter a keyword. + Add Filter ✖																
Index	Name	Descri...	Tag	Source...	Destin...	Source...	Destin...	User	Service	Applic...	Schedule	Action	Conten...	Hits	Enable	Edit
1	default	This is t...		any	any	any	any	any	any	any	any	Deny		104 R...	🟢	🛠

Chapter
06

Configuring Addresses and Address Groups on the Web UI

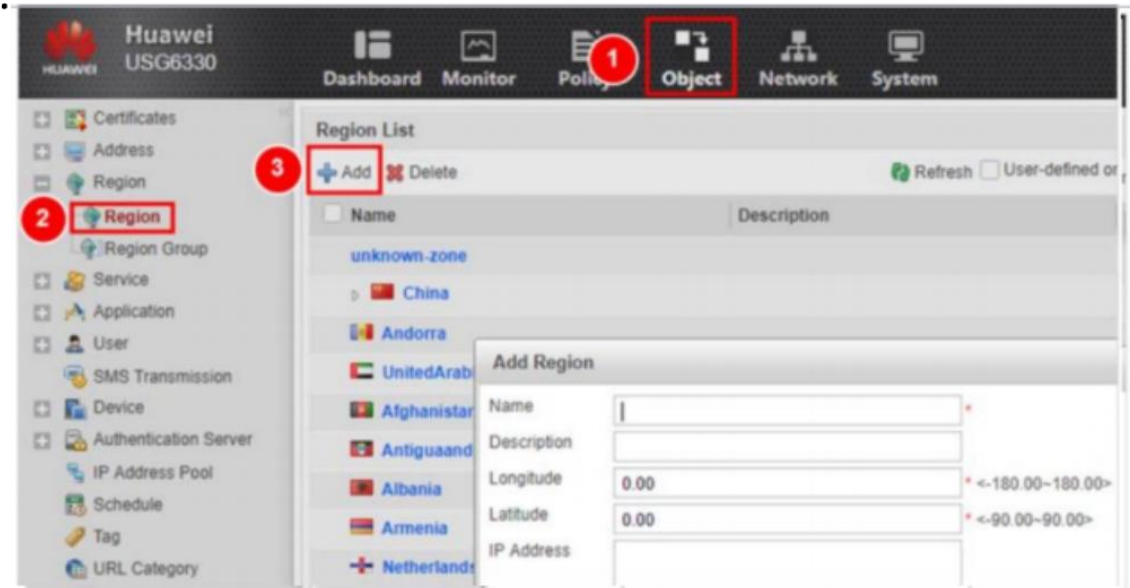
- An address object is a set of IPv4/IPv6 addresses or MAC addresses. An address group is a set of address objects.
- An address object contains one or more IPv4/IPv6 addresses or MAC addresses. It is like a basic component and can be referenced by different policies (such as security policies and NAT policies).
- Procedure for configuring the address and address group on the web UI:
 - Choose Object > Address > Address (or Address Group).
 - Click Add and set the parameters of the address (or address group).
 - Click OK. The created address (or address group) is displayed.



Chapter 06

Configuring Regions and Region Groups on the Web UI

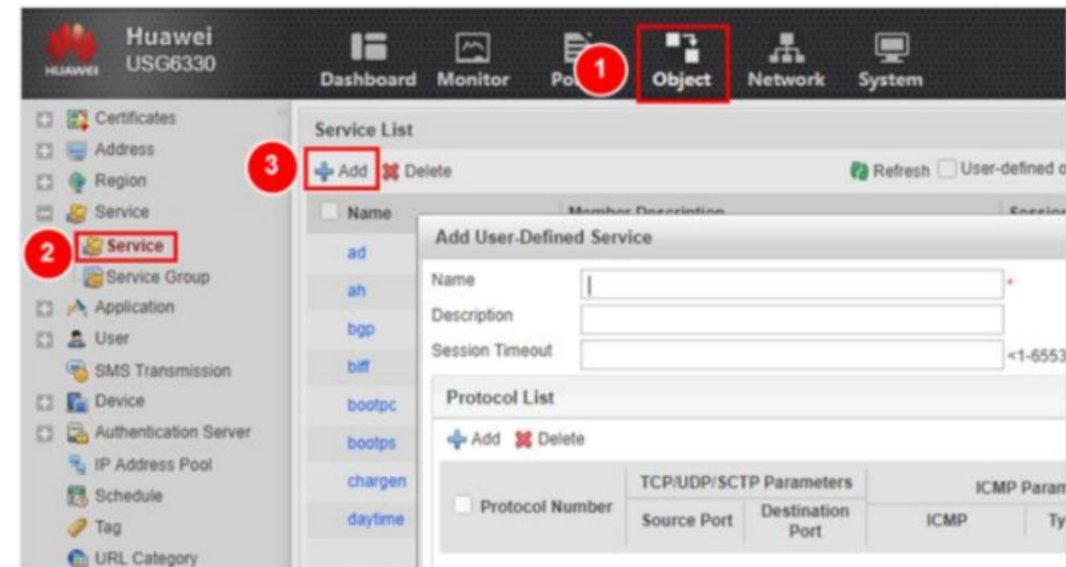
- A region is a set of public IP addresses in a certain area.
- A region group contains multiple regions or region groups. Region groups can be configured and referenced by policies.
- Procedure for configuring the region and region group on the web UI:
 - Choose Object > Region > Region (or Region Group).
 - Click Add to set the parameters of the region (or region group).
 - Click OK. The created region (or region group) is displayed.



Chapter
06

Configuring Services and Service Groups

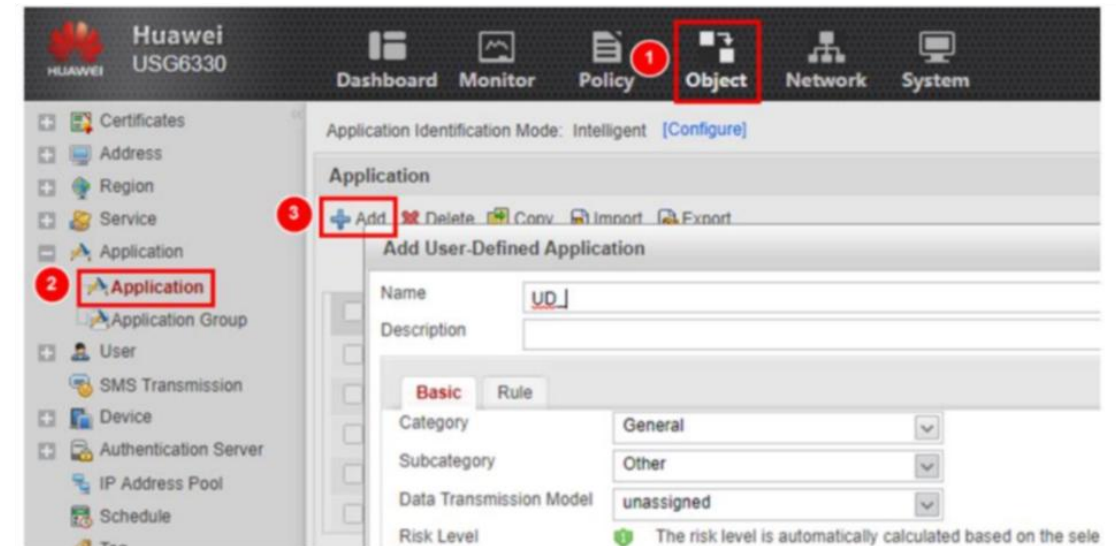
- A service is a type of application protocol determined by a protocol type and a port number. A service group is a collection of services and service groups.
- **Predefined service:** A service that has been preset in the system by default and can be selected directly.
- **User-defined service:** A service defined by specifying certain information including the application protocol type (such as TCP, UDP, or ICMP) and port number.
- Predefined services are generally well-known protocols, such as HTTP, FTP, and Telnet. Predefined services cannot be deleted.
- Procedure for configuring services and service groups on the web UI:
 - Choose Object > Service > Service (or Service Group).
 - Click Add and set the parameters of the user-defined service.
 - Click OK. The created service (or service group) is displayed.



Chapter
06

Configuring Applications and Application Groups on the Web UI

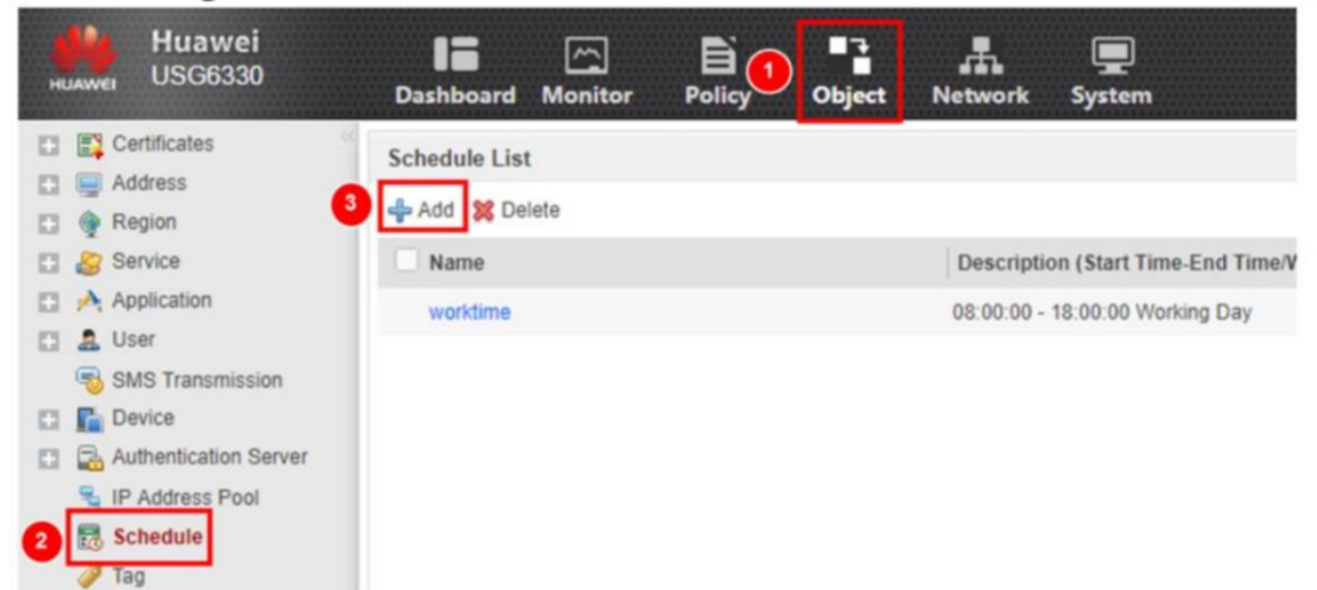
- Applications are computer programs used for a special purpose or performing a special task. An application group is a collection of applications.
- Procedure for configuring applications and application groups on the web UI:
 - ❑ Choose Object > Application > Application (or Application Group).
 - ❑ Click Add and set the parameters of the user-defined application.
 - ❑ Click OK. The created application (or application group) is displayed.



Chapter
06

Configuring a Schedule on the Web UI

- A schedule can be referenced by a policy to match the traffic passing through a firewall during the schedule.
- Procedure for configuring a schedule on the web UI:
 - Choose Object > Schedule.
 - Click Add.
 - Enter the name of the schedule list to be created.
 - Add schedules to the list.
 - Click OK.



Chapter
06

Configuring a Security Policy on the Web UI

- You can reference existing objects in a security policy.
- Procedure for configuring a security policy on the web UI:
 - ❑ Choose Policy > Security Policy > Security Policy.
 - ❑ Click Add.
 - ❑ Enter the name and description of the security policy.
 - ❑ Define the matching conditions of the security policy.
 - ❑ Set the action of the security policy.
 - ❑ Configure the security policy to reference content security profiles.
 - ❑ Click OK.

The screenshot shows the 'Add Security Policy' web UI form. It includes a note at the top: 'Note: You can use a policy template to quickly define the required policy. [Select Template]'. There is a 'Switch Source and Destination' button. The form fields are as follows:

- Name: Text input field.
- Description: Text input field.
- Policy Group: Dropdown menu with '-- NONE --' selected.
- Tag: Text input field with placeholder 'Select or enter a tag.'
- Source Zone: Dropdown menu with placeholder 'Select a source zone.' and a '[Multiple]' link.
- Destination Zone: Dropdown menu with placeholder 'Select a destination zone.' and a '[Multiple]' link.
- Source Address/Region: Text input field with placeholder 'Select or enter an address.'
- Destination Address/Region: Text input field with placeholder 'Select or enter an address.'
- User: Text input field with placeholder 'Select or enter a user name.' and a '[Multiple]' link.
- Access Mode: Text input field with placeholder 'Select an access mode.'
- Device: Text input field with placeholder 'Select or enter a device.'
- Service: Text input field with placeholder 'Select or enter a service.'
- Application: Text input field with placeholder 'Select or enter an application.' and a '[Multiple]' link.

Below the Application field, there is a note: 'Specifying application will automatically enable the SA function. This function reduces system performance.'

At the bottom, there are two more fields:

- URL Category: Text input field with placeholder 'Select or enter a uri category.' and a '[Multiple]' link.
- Schedule: Dropdown menu with placeholder 'Select a time range.'

At the bottom right, there are three buttons: 'OK', 'OK and Copy', and 'Cancel'.

Chapter
06

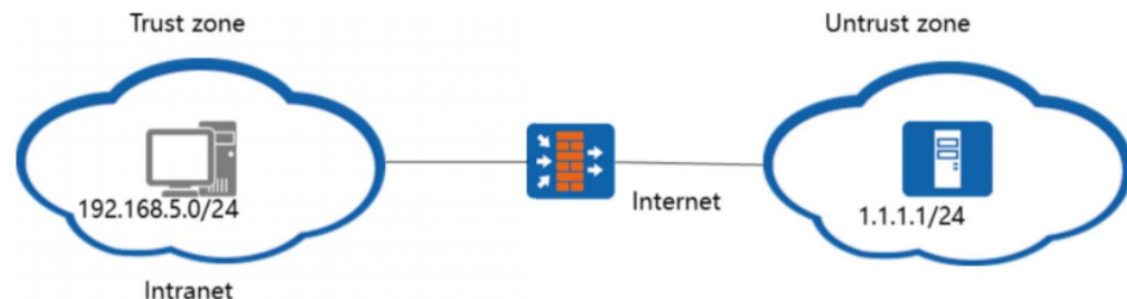
Example for Configuring Security Policies

- Networking Requirements

- On an enterprise network, PCs in the 192.168.5.0/24 network segment are allowed to access the Internet, but PCs at 192.168.5.2, 192.168.5.3, and 192.168.5.6 in this network segment are not allowed to access the Internet.

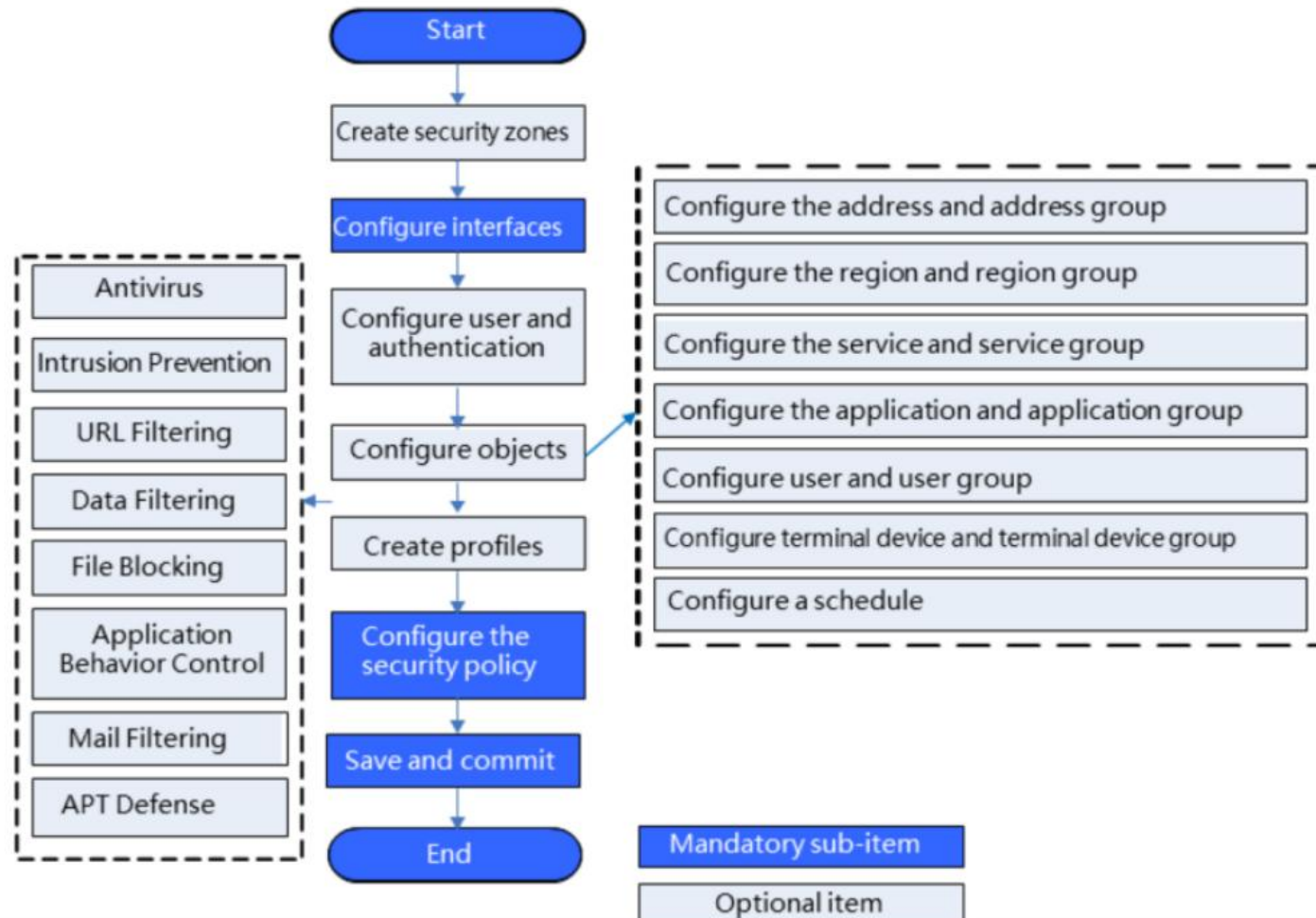
- Configuration roadmap:

- Plan security policies: The network segment 192.168.5.0/24 is permitted, but several IP addresses within the range are denied. In this case, configure two forwarding policies. The first forwarding policy denies the specific IP addresses and the second forwarding policy allows the entire network segment. If the configuration sequence is reversed, the special IP addresses will match the permit policy and the packets pass through the firewall.
- Plan address groups: It is required to control access permissions by IP address. Specify IP addresses as the matching conditions in the forwarding policies. Consecutive address segments can be directly configured in a policy. For inconsecutive addresses, you are advised to add them to an address group, so that the addresses can be controlled in a unified manner and the address group can be referenced by policies. In this example, the special IP addresses can be configured as an address group.
- Configure forwarding policies to control Internet access permissions.



Chapter
06

Security Policy Configuration Process



Security Policy Configuration Process

- **Security policy configuration roadmap:**

- ❑ **Determine security zones, connect interfaces, and assign the interfaces to the security zones.**
- ❑ **Classify employees by source IP address or user.**
- ❑ **Use security policies to determine the permissions of user groups and then those of privileged users. You must specify the source security zones and addresses of users, destination security zones and addresses of users, services and applications that the users can access, and schedules in which the policies take effect. To allow a certain type of network access, set the action of the security policy to permit. To disable network access, set the action of the security policy to deny.**
- ❑ **Determine which types of traffic needs content security inspection and what items need to be inspected.**
- ❑ **List the parameters in the security policies, sort the policies from the most specific to the least specific, and configure security policies in this order.**

Chapter
06

Key Configuration (Commands)

- Create a security policy rule that denies the access of special IP addresses to the Internet.

```
[NGFW]security-policy
[NGFW-policy-security]rule name celue
[NGFW-policy-security-rule-celue]source-zone trust
[NGFW-policy-security-rule-celue]destination-zone untrust
[NGFW-policy-security-rule-celue]source-address 192.168.5.2 32
[NGFW-policy-security-rule-celue]source-address 192.168.5.3 32
[NGFW-policy-security-rule-celue]source-address 192.168.5.6 32
[NGFW-policy-security-rule-celue]action deny
```

- Create a security policy rule that allows the 192.168.5.0/24 network segment to access the Internet.

```
[NGFW]security-policy
[NGFW-policy-security]rule name celue2
[NGFW-policy-security-rule-celue2]source-zone trust
[NGFW-policy-security-rule-celue2]destination-zone untrust
[NGFW-policy-security-rule-celue2]source-address 192.168.5.0 24
[NGFW-policy-security-rule-celue2]action permit
```

- The configuration of the ipdeny address group is as follows:
 - ❑ [sysname] ip address-set ip deny type object
 - ❑ [sysname-object-address-set-ip_deny] address 0 192.168.5.2 0
 - ❑ [sysname-object-address-set-ip_deny] address 1 192.168.5.3 0
 - ❑ [sysname-object-address-set-ip_deny] address 2 192.168.5.6 0

Chapter
06

Key Configuration on the Web UI (1)

- Configure an address group named ip deny.
 - Configure address group ip deny and add the IP addresses that are not allowed to access the Internet to this address group.
- ☐ Choose Object > Address > Address.
 - ☐ Click Add and set address parameters.
 - ☐ Click OK. The added addresses are displayed.

Add Address Group

Name:

Description:

Reference Address or Address Group:

IP Address/Range or MAC Address:

Available:

Selected:

Enter each IP Address/Range or MAC Address on a separate line. For example:
10.10.1.2
10.10.1.2/255.255.255.0
10.10.1.2/32
10.10.1.2/0.0.0.255

Chapter
06

Key Configuration on the Web UI (2)

- Configure a security policy to deny the access of the addresses in address group ipdeny to the Internet.
- Configure a security policy for denying the access from the IP addresses in address group ip deny to the Internet Set Source Address to ip deny and Action to Deny.

Note: You can use a policy template to quickly define the required policy. [Select Template] Switch Source and Destination (?)

Name: policy_deny

Description:

Policy Group: -- NONE --

Tag: Select or enter a tag.

Source Zone: trust [Multiple]

Destination Zone: untrust [Multiple]

Source Address/Region: ip_deny x

Destination Address/Region: Select or enter an address.

User: Select or enter a user name. [Multiple]

Access Mode: Select an access mode.

Device: Select or enter a device.

Service: Select or enter a service.

Application: Select or enter an application. [Multiple]

Specifying application will automatically enable the SA function. This function reduces system performance.

URL Category: Select or enter a url category. [Multiple]

Schedule: Select a time range.

Action: ☐ Permit ☒ Deny

Chapter
06

Key Configuration on the Web UI (3)

- Configure a security policy to allow access from the 192.168.5.0/24 network segment to the Internet.
- Configure a security policy to allow access from the 192.168.5.0/24 network segment to the Internet. Set Source Address to 192.168.5.0/24 and Action to Permit.

Add Security Policy

Note: You can use a policy template to quickly define the required policy. [Select Template] [Switch Source and Destination](#)

Name: policy_permit

Description:

Policy Group: -- NONE --

Tag: Select or enter a tag.

Source Zone: trust [Multiple]

Destination Zone: untrust [Multiple]

Source Address/Region: 192.168.5.0/24 x

Destination Address/Region: Select or enter an address.

User: Select or enter a user name. [Multiple]

Access Mode: Select an access mode.

Device: Select or enter a device.

Service: Select or enter a service.

Application: Select or enter an application. [Multiple]

Specifying application will automatically enable the SA function. This function reduces system performance.

URL Category: Select or enter a url category. [Multiple]

Schedule: Select a time range.

Action: ☒ Permit ☐ Deny

Chapter
06

Multi-channel Protocol Technology

- **Single-channel protocol:** uses only one port during communication. For example, WWW uses only port 80.
- **Multi-channel protocol:** uses two or more ports for communication. For example, FTP passive mode uses port 21 and a random port.

How to only use packet filtering methods to precisely define the ports used by multi channel protocols?

For protocols that use random ports, pure packet filtering cannot define data flows.

- Most multimedia application protocols (such as H.323 and SIP), FTP, and NetMeeting use prescribed ports to initialize a control connection and then dynamically select a port for data transmission. Port selection is unpredictable. An application may use more than one port at a time. Packet filtering firewalls can use ACLs to match applications of single channel protocols to prevent network attacks. However, ACLs can block only applications using fixed ports. Multi-channel protocol applications that use random ports bring security risks.

Chapter
06

ASPF Overview

- **Application Specific Packet Filter (ASPF)**, as an advanced filtering technology, checks application-layer protocol information and monitors the status of the connected application-layer protocol. For all connections of a specified application protocol, ASPF maintains status information and dynamically determines whether to permit data packets to pass through the firewall or discard data packets.



Monitor communication packets.



Dynamically create and delete filtering rules.



Chapter
06

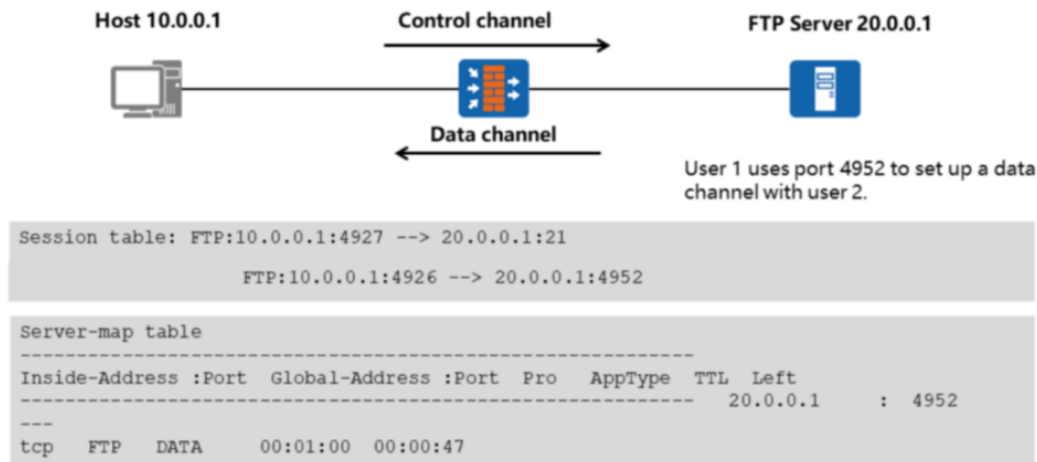
Firewall Interzone Forwarding

- ASPF maintains information about connections in its own data structure and uses the information to create temporary rules. ASPF stores status information that cannot be stored in ACLs. A firewall checks each packet in a data flow to ensure that the packet status and packet comply with user-defined security rules. The status information of connections is used to intelligently permit or deny packets. When a session is closed, the ASPF session management module deletes this session from its session table and closes it in the session table of the firewall.
- For TCP connections, ASPF can dynamically detect TCP three-way handshake and the handshake for connection termination to ensure normal TCP access. The packets of incomplete TCP handshake connections are rejected.
- UDP is a connectionless protocol. Therefore, there is no UDP connection. ASPF is connection-based. It checks the source IP address, destination IP address, and port of a UDP packet and determines whether the packet is similar to other UDP packets received within a specific period. If the packet is similar, ASPF determines that these packets are over the same connection.
- ACL-based IP packet filtering technology is widely used for access control. This technology is simple but lacks flexibility and is unable to competently protect complex networks. For example, for the multi-channel protocols using FTP for communication, it is difficult to configure the rules of the firewall.
- ASPF enables the firewall to support the protocols of multiple data connections over one control channel. It also supports various security policies in very complex application scenarios. ASPF monitors the port used by each application connection, opens an appropriate path to permit the data in a session, and closes this path at the end of the session. In this way, the firewall can control the access of applications using dynamic ports.

Chapter
06

ASPF Supports Multi-channel Protocols

- ASPF is used to filter packets at the application layer.
- In a multi-channel protocol, for example, FTP, the control channel is separated from the data channel. The data channel is dynamically negotiated by control packets. To prevent the data channel from being disconnected by other rules, such as ACLs, a channel must be temporarily enabled. This is why the server map is applied.
- FTP establishes a TCP control channel with predefined ports and a dynamically negotiated TCP data channel. For a common packet filtering firewall, you cannot obtain the port number of the data channel when configuring security policies, and therefore cannot determine the ingress of the data channel. In this case, precise security policies cannot be configured. ASPF resolves this problem. It detects application-layer information and dynamically creates and deletes temporary rules based on packet content to allow or deny packets.

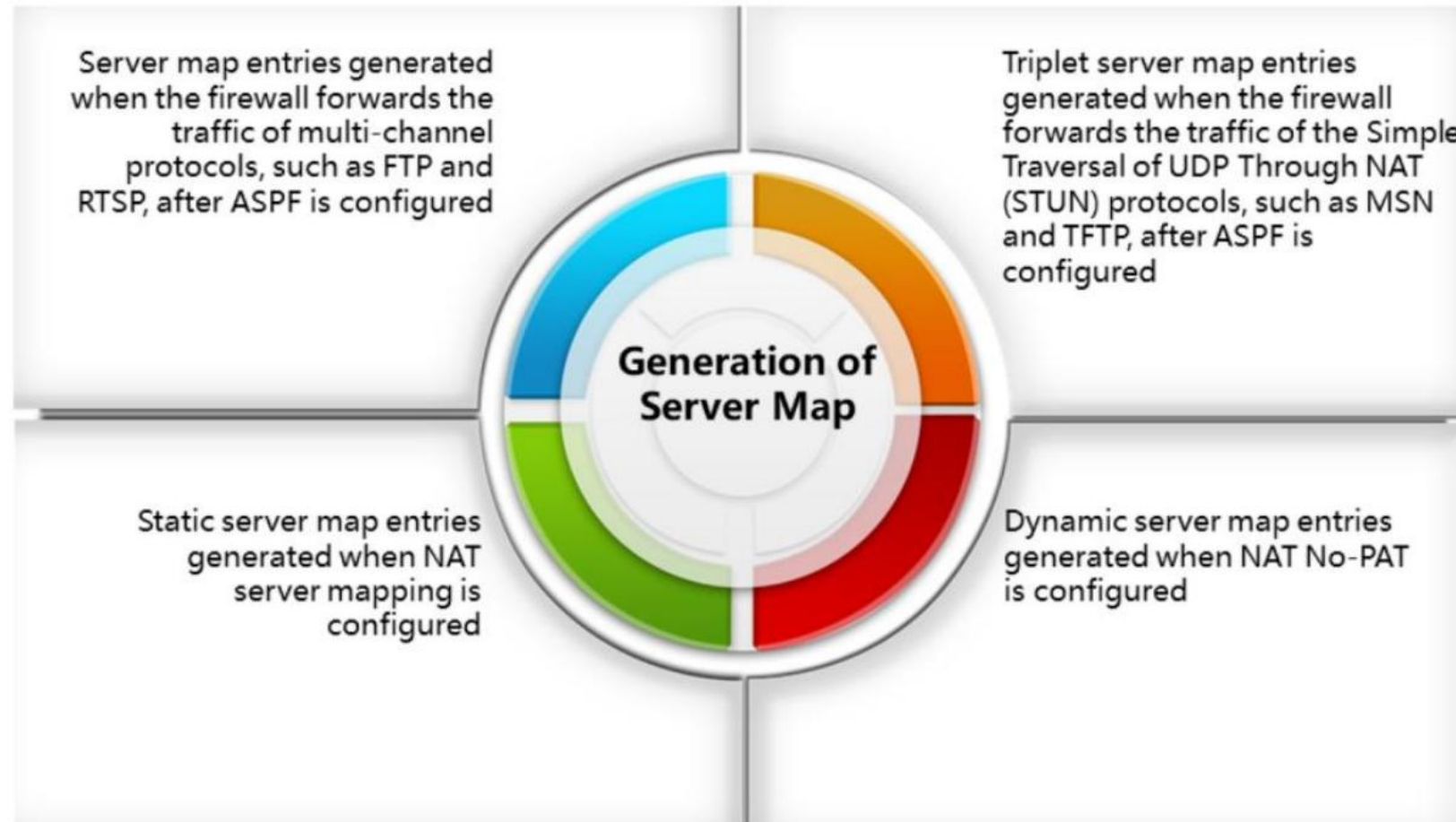


ASPF Supports Multi-channel Protocols

- According to the figure, the server map entry is generated during the dynamic detection of the FTP control channel. When a packet passes the firewall, ASPF compares the packet with the specified access rules. If the rules permit, the packet is checked; otherwise, the packet is discarded. If the packet is used to establish a new control or data connection, ASPF dynamically creates a server map entry. Return packets can pass through the firewall only when they have a matching server map entry. When processing return packets, the firewall updates the status table. When a connection is closed or times out, the corresponding status table is deleted to block unauthorized packets. Therefore the ASPF technology can accurately protect the network even in complicated application scenarios.
- The server map is a mapping relationship. If a data connection matches a dynamic server map entry, the firewall does not need to search for a packet filtering policy. This mechanism ensures normal forwarding of some special applications. In another case, if a data connection matches the server map table, the IP address and port number in the packet are translated.
- The server map is used only for checking the first packet. After a connection is established, packets are forwarded based on the session table.

Chapter
06

Generation of Server Map



Chapter
06

Generation of Server Map

- Currently, the firewall generates server map entries in the following situations: server map entries generated when the firewall forwards the traffic of multi-channel protocols, such as FTP and RTSP, after ASPF is configured; triplet server map entries generated when the firewall forwards the traffic of the Simple Traversal of UDP Through NAT (STUN) protocols, such as MSN and TFTP, after ASPF is configured; static server map entries generated when NAT server mapping is configured; dynamic server map entries generated when NAT No-PAT is configured; dynamic server map entries generated when NAT full-cone is configured; dynamic server map entries generated when PCP is configured; static server map entries generated when server load balancing (SLB) is configured; dynamic server map entries generated when NAT Server is configured in DS- Lite scenarios; static server map entries generated when static NAT64 is configured.
- The data connection of a multi-channel protocol is negotiated on the control connection. Therefore, source and destination ports of the data connection are dynamically negotiated. After ASPF is configured, the firewall identifies the negotiation of the control channel, and dynamically creates a server map entry according to the address information in the key packet payload being queried during the connection initiation of the data channel. The server map entry contains information about the negotiated data channel.

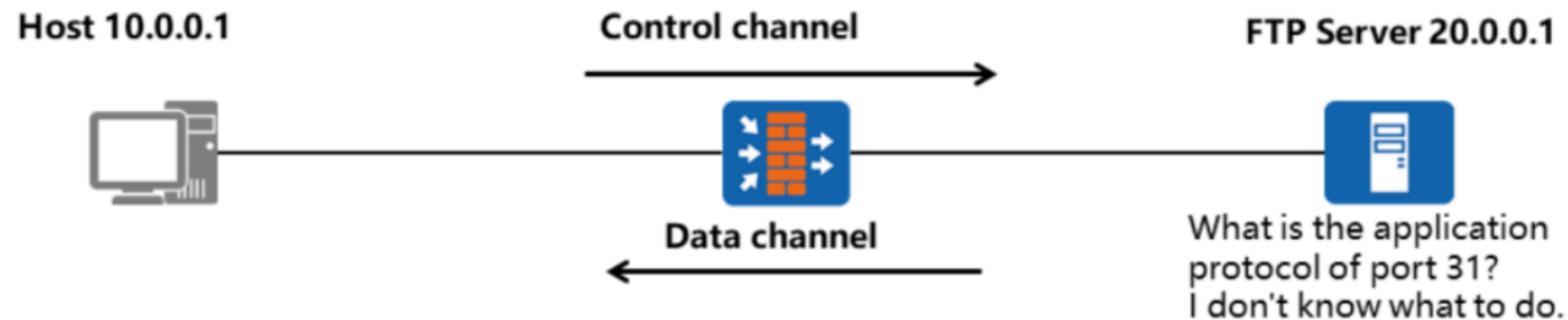
Chapter
06

Generation of Server Map

- After an MSN user logs in, the IP address and port of the user are determined, but those of the other party that may initiate a connection to the user are unknown. If you configure ASPF, the firewall records the IP address and port of the user and generates a dynamic server map entry when the MSN user is connected to the server. The server map entry contains only triplet information: IP address, port number, and protocol number of one communications party. In this way, other users can directly adopt the IP address and port to communicate with this user.
- After NAT Server is configured, Internet users can initiate access requests to the intranet server. The IP addresses and ports of the users are unknown, but the IP address of the intranet server and the port are known. Therefore, after NAT Server is successfully configured, the firewall automatically generates the server map entry to save the mapping relationship between the public and private IP addresses. The firewall translates the IP address of the packet and forwards the packet according to the mapping relationship. A pair of forward and reverse static server map entries are generated for each valid NAT Server configuration. For SLB, as multiple intranet servers use the same public IP address, the firewall creates server map entries similar to those of NAT Server. If the number of intranet servers is N, the firewall creates one server map entry for forward traffic and N server map entries for reverse traffic.
- If you configure NAT and specify the No-PAT parameter, the firewall translates only the IP addresses but not the port numbers. All port numbers used by private IP addresses are mapped to the port number used by the public address. Internet users can initiate connections to any port used by an intranet user. After NAT No-PAT is configured, the firewall creates server map entries for the data flows to maintain the mapping between the private and public IP addresses. Then the firewall translates IP addresses and forwards packets according to the mappings.

Support for Multi-channel Protocols by Port Identification

- Port identification maps non-standard protocol ports to identifiable application protocol ports.



- Configure a basic ACL.

```
[NGFW]acl 2000  
[NGFW-acl-basic-2000]rule permit source 20.0.0.1 0
```

- Configure port identification (or port mapping).

```
[NGFW]port-mapping FTP port 31 acl 2000
```

Support for Multi-channel Protocols by Port Identification

- Port identification, also called port mapping, is used by the firewall to identify application-layer protocol packets that use non-standard ports. Port mapping supports the following application-layer protocols: FTP, HTTP, RTSP, PPTP, MGCP, MMS, SMTP, H323, SIP, and SQLNET.
- Port mapping is implemented based on ACLs. Only the packets matching an ACL rule are mapped. Port mapping uses basic ACLs (ACLs 2000 to 2999). In ACL-based packet filtering, the firewall matches the destination IP addresses of packets with the source IP addresses in basic ACLs.
- An ACL is a collection of sequential rules used by a device to filter network traffic. Each rule contains a filter element that is based on criteria such as the source IP address, destination IP address, and port number of a packet. An ACL classifies packets based on rules. After the rules are applied to a router, the router determines whether a packet is permitted or denied in accordance with these rules.

Support for Multi-channel Protocols by Port Identification

- **ACLs are classified into the following types:**
 - ❑ **Basic ACLs (2000 to 2999):** A basic ACL matches traffic only by source IP address and schedule. It applies to simple matching scenarios.
 - ❑ **Advanced ACLs (3000 to 3999):** Traffic is matched by source IP address, destination IP address, ToS, schedule, protocol type, priority, ICMP packet type, and ICMP packet code. In most functions, advanced ACLs can be used for accurate traffic matching.
 - ❑ **MAC address-based ACLs (4000 to 4999):** Traffic is matched by source MAC address, destination MAC address, CoS, and protocol code.

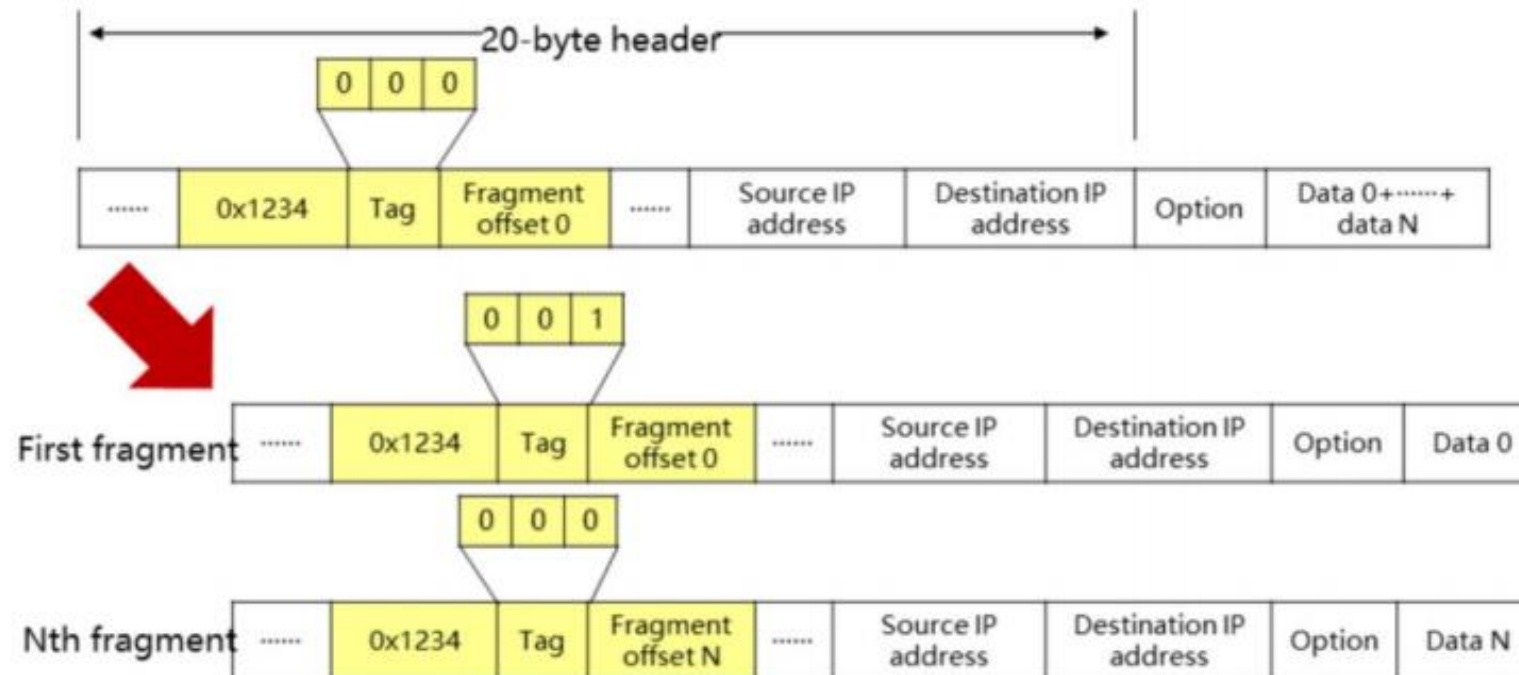
Support for Multi-channel Protocols by Port Identification

- **Hardware packet filtering ACLs (9000 to 9499):** After a hardware packet filtering ACL is delivered to an interface card, the interface card filters packets using hardware, which is faster than common software-based packet filtering and consumes less system resources. Hardware packet filtering ACLs can match traffic based on the source IP address, destination IP address, source MAC address, destination MAC address, CoS, and protocol type.
- Port mapping applies only to the data within an interzone; therefore, when configuring port mapping, you must configure security zones and the interzone.
- **Thinking:** What is the application system object matching ACLs?

Chapter
06

Fragment cache

- The fragment cache function is used to cache fragments that arrive before the first fragment in the flow. This function prevents the firewall from discarding fragments.



Fragment cache

- When a network device transmits a packet, if the Maximum Transfer Unit (MTU) configured on the device is shorter than the length of the packet, the packet is fragmented before transmission. In an ideal case, fragment packets are transmitted in a fixed order. During actual transmission, the first fragment may not be the first to reach the firewall. In this case, the firewall discards the fragmented packet. To ensure session continuity, the firewall can cache fragments by default. The firewall caches the fragments that reach the firewall before the first fragment to the fragment hash list. When the first fragment arrives, the firewall creates a session for the fragmented packet and forwards all the fragments. If the first fragment does not arrive within a specified period, the firewall discards the fragments in the fragment hash list.
- In VPN applications (such as IPSec and GRE), because the firewall can perform further processing only after it reassembles, and decrypts or decapsulates fragmented packets. Therefore, the fragment cache function must be configured on the firewall to reassemble packets, so that the packets can be encrypted or decrypted. In NAT application, the firewall can translate the IP address of a fragmented packet only after it reassembles the fragments. Therefore, the fragment cache function is also required.

Fragment cache

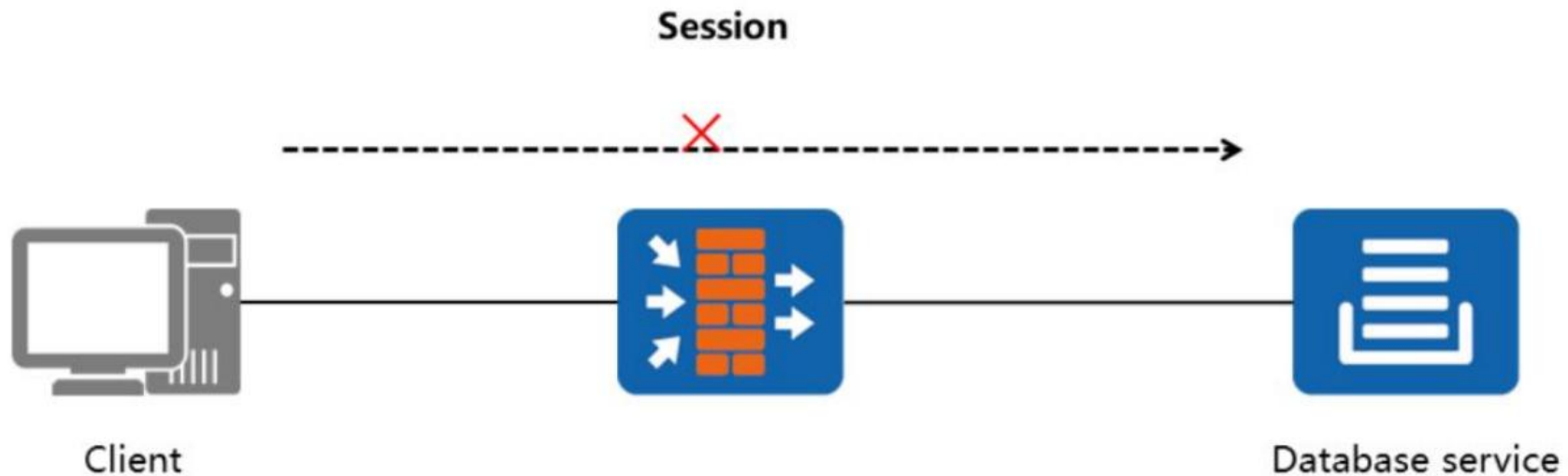
- The function of directly forwarding fragments applies when NAT is not performed. After this function is enabled, the firewall directly forwards received fragments without creating any session.
- Set the aging time for fragment cache.
 - Firewall session aging-time fragment interval (1-40000)
- Enable or disable the function of directly forwarding fragments.
 - Firewall fragment-forward enable/disable

Chapter
06

Persistent Connection

- Why are persistent connections required?
 - Aging mechanism of the firewall session table
 - Problems caused by the session aging mechanism to special services

If no data is transmitted within the session aging time, the session is disconnected.



Persistent Connection

- If the interval for two consecutive packets of a TCP session reaching the firewall is longer than the aging time of the session, the firewall deletes the session information from the session table. In this case, after subsequent packets reach the firewall, the firewall discards the packets. As a result, the connection is interrupted. Some services require persistent sessions. To solve this problem, the firewall supports the configuration of persistent connections in the interzone. By referencing ACLs to define data flow rules, you can set long aging time for the sessions of the packets that match the ACL rules to ensure the normal use of the sessions. The default aging time of a persistent connection is 168 hours.
- The firewall supports the persistent connection function only for TCP packets.

Persistent Connection

- When stateful inspection is disabled, the firewall also creates session entries for non-first packets. In this case, you do not need to enable the persistent connection function.
- Set aging time for a persistent connection.
 - ❑ Firewall long-link aging-time time
- Enable persistent connection.
 - ❑ Firewall interzone zone-name1 zone-name2
 - ❑ lonk-link acl-number {inbound | outbound }



Thank You