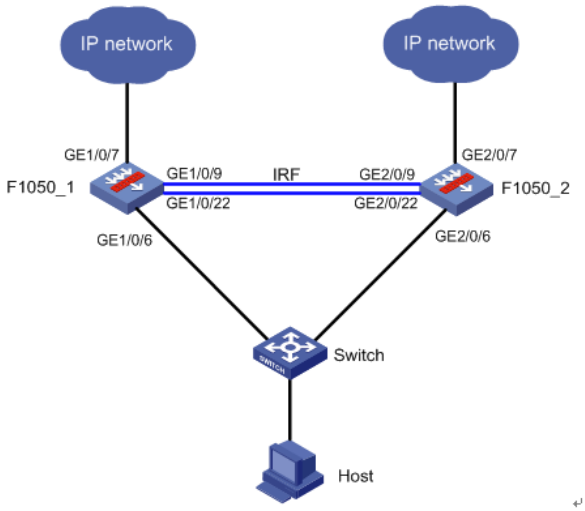
NGFW device dual-active egress gateway typical configuration

Security 龚训杰 2021-02-02 Published

Network Topology

As shown in Figure 1, two F1050s form an IRF. Intranet users aggregate HASH through the firewall"s downlink and are distributed to two devices. The firewall is routed to the telecommunications network and China Unicom network through link load balancing technology. Configure on F1050 Link aggrega tion is locally preferred, and local forwarding traffic is prioritized from the device to avoid horizontal tra ffic. Because there are asymmetric scenarios, you need to configure the session hot backup function.



• Establish IRF between two F1050s.

• In order to prevent the IRF from splitting due to an IRF link failure, two IRFs with conflicting configur ations are generated on the network, and the MAD detection function needs to be enabled. Detect G E1/0/4 of F1050_1 and GE2/0/4 of F1050_2 BFD MAD.

• Configure GE1/0/6 of F1050_1 and GE2/0/6 of F1050_2 as Layer 3 aggregation ports. GE1/0/7 of F1050_1 is configured as a telecom network outgoing interface and added to aggregation group 2, and GE2/0/7 of F1050_2 is configured as a Unicom network outgoing interface, and it is also added t o aggregation group 3.

• Configure link load balancing on the firewall to load-share intranet traffic between the two links.

Configuration Steps

Configuration Notes:

Pay attention to the configuration sequence when configuring the stack for the F1050. After saving th e configuration, activate the stack port configuration.

F1050 IRF

IRF configuration (Two F1050s can be connected through multiple IRF ports. Take GE1/0/9~ GE 2/0/9 and GE1/0/22 ~ GE2/0/22 as examples below)

F1050_1 configuration

Configure member number and priority

system-view

[F1050_1] irf member 1 priority 32

Configure F1050_1, configure IRF port 1/1, bind it to physical ports GE1/0/9 and GE1/0/22, save th e configuration, and activate the configuration under the IRF port.

[F1050_1] interface GigabitEthernet 1/0/9

[F1050_1-GigabitEthernet1/0/9] shutdown

[F1050_1-GigabitEthernet1/0/9] quit

[F1050_1] interface GigabitEthernet 1/0/22

[F1050_1-GigabitEthernet1/0/22] shutdown

[F1050_1-GigabitEthernet1/0/22] quit

[F1050_1] irf-port 1/1

[F1050_1-irf-port1/1] port group interface GigabitEthernet 1/0/9

[F1050_1-irf-port1/1] port group interface GigabitEthernet 1/0/22

[1050_1-irf-port1/1] quit

[F1050_1] interface GigabitEthernet 1/0/9

[F1050_1-GigabitEthernet1/0/9] undo shutdown

[F1050_1-GigabitEthernet1/0/9] quit

[F1050_1] interface GigabitEthernet 1/0/22

[F1050_1-GigabitEthernet1/0/22] undo shutdown

[F1050_1-GigabitEthernet1/0/22] quit

[F1050_1] save

[F1050_1] irf-port-configuration active

(1) Configuration of F1050_2

Configure member number

system-view

[F1050_2] irf member 1 renumber 2

Warning: Renumbering the member ID may result in configuration change or loss. Continue? [Y/N]:y

[F1050_2] quit

reboot

F1050_2 After restarting, log in to the device and set the IRF priority.

system-view

[F1050_2] irf member 2 priority 1

Configure IRF port 2/2 and bind it to physical ports GE2/0/9 and GE2/0/22, save the configuration, a nd activate the configuration under the IRF port.

[F1050_2] interface GigabitEthernet 2/0/9

[F1050_2-GigabitEthernet2/0/9] shutdown

[F1050_2-GigabitEthernet2/0/9] quit

[F1050_2] interface GigabitEthernet 2/0/22

[F1050_2-GigabitEthernet2/0/22] shutdown

[F1050_2-GigabitEthernet2/0/22] quit

[F1050_2] irf-port 2/2

[F1050_2-irf-port2/2] port group interface GigabitEthernet 2/0/9

[F1050_2-irf-port2/2] port group interface GigabitEthernet 2/0/22

[F1050_2-irf-port2/2] quit

[F1050_2] interface GigabitEthernet 2/0/9

[F1050_2-GigabitEthernet2/0/9] undo shutdown

[F1050_2-GigabitEthernet2/0/9] quit

[F1050_2] interface GigabitEthernet 2/0/22

[F1050_2-GigabitEthernet2/0/22] undo shutdown

[F1050_2-GigabitEthernet2/0/22] quit

[F1050_2] save

[F1050_2] irf-port-configuration active

F1050 aggregate interface configuration

F1050 is configured with a three-layer aggregation port in the downstream to split the downstream applicat
ion traffic to two devices.

Key Configuration

Enable the aggregation acceleration function, which needs to be configured in dual main mode.

[F1050_1] link-aggregation global-forwarding-acceleration enable

GE1/0/6 of F1050_1 and GE2/0/6 of F1050_2 form the aggregation port RAGG1.

[F1050_1] interface Route-Aggregation 1

[F1050_1-Route-Aggregation1] quit

[F1050_1] interface GigabitEthernet 1/0/6

[F1050_1-GigabitEthernet1/0/6] port link-aggregation group 1

[F1050_1-GigabitEthernet1/0/6] quit

[F1050_1] interface GigabitEthernet 2/0/6

[F1050_1-GigabitEthernet2/0/6] port link-aggregation group 1

[F1050_1-GigabitEthernet2/0/6] quit

Configure the IP address of the aggregation port BAGG1.

[F1050_1] interface Route-Aggregation 1

[F1050_1-Route-Aggregation1] ip address 192.168.1.254 24

[F1050_1-Route-Aggregation1] quit

Add the aggregation port to the security zone trust.

[F1050_1] security-zone name trust

[F1050_1-security-zone-Trust] import interface Route-Aggregation 1

[F1050_1-security-zone-Trust] quit

F1050 link load balancing configuration

Create link group lg1 of isp1 where Link1 and Link2 are located, and configure the algorithm to rotate

[F1050_1] loadbalance link-group lg1

[F1050_1-lb-lgroup-lg1] predictor round-robin

[F1050_1-lb-lgroup-lg1] transparent enable

[F1050_1-lb-lgroup-lg1] quit

Create links Link1 and Link2 and belong to link group lg1.

[F1050_1] loadbalance link link-1

[F1050_1-lb-link-link-1] router ip 10.152.2.254 //电信

[F1050_1-lb-link-link-1] link-group lg1

[F1050_1-lb-link-link-1] quit

[F1050_1] loadbalance link link-2

[F1050_1-lb-link-link-2] router ip 10.152.3.254 //联通

[F1050_1-lb-link-link-2] link-group lg1

[F1050_1-lb-link-link-2] quit

Create a NAT address pool address globally.

[F1050_1] nat outbound address-group 1

[F1050_1-address-group-1] address 10.153.1.10 10.153.1.10

[F1050_1-address-group-1] quit

[F1050_1] nat outbound address-group 2

[F1050_1-address-group-1] address 10.154.1.10 10.154.1.10

[F1050_1-address-group-1] quit

NAT outbound is enabled on the corresponding interfaces of link link-1 and link-2, referencing address pool addresses 1, 2 respectively

[F1050_1] interface Route-Aggregation 2

[F1050_1-Route-Aggregation2] nat outbound address-group 1

[F1050_1-Route-Aggregation2] quit

[F1050_1] interface Route-Aggregation 3

[F1050_1-Route-Aggregation3] nat outbound address-group 2

[F1050_1-Route-Aggregation2] quit

Enable slot1 NAT port load sharing function globally. In the load sharing scenario of dual-system ho
t backup, after the NAT port load sharing function is enabled, the two devices each get half of the port block resources, so that the same private network IP address can exclusively occupy certain port res
ources on different member devices, avoiding port allocation conflict. When it is not turned on, there may be multiple private network addresses that use the same port after NAT translation, causing ses
sion conflicts.

[F1050_1] nat port-load-balance enable slot 1

Create a traffic classification class-1, based on the application group app-1 and ACL 3001 to match the HTTP traffic whose source IP is the IP address of the 192.168.0.0/16 network segment.。

Verify configuration

(1) View the HAF information formed by two firewalls

display hf

MemberID Role Priority CPU-Mac Description

1 Master 32 50da-00eb-7ba1 ---

2 Standby 1 50da-00e8-7bd3 ---

* indicates the device is the master.

+ indicates the device through which the user logs in.

The bridge MAC of the HAF is: 50da-00eb-7b9f

Auto upgrade : yes

Mac persistent : 6 min

Domain ID : 30

GE1/0/6 S 32768 1

GE2/0/6 S 32768 1

(2) View the status of the aggregation port

display link-aggregation verbose Route-Aggregation 1

Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing

Port Status: S -- Selected, U -- Unselected, I -- Individual

Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,

D -- Synchronization, E -- Collecting, F -- Distributing,

G -- Defaulted, H -- Expired

Aggregate Interface: Route-Aggregation1

Aggregation Mode: Static

Loadsharing Type: Shar

Port Status Priority Oper-Key

GE1/0/6 S 32768 1

GE2/0/6 S 32768 1

(3) View LLB virtual service status

display virtual-server name vs

Virtual server: vs

Description:

Type: LINK-IP

State: Active

VPN instance:

Virtual IPv4 address: 0.0.0.0

Virtual IPv6 address: --

Port: 0

Primary link group:

Backup link group:

Sticky:

LB policy: policy-1

LB limit policy:

Connection limit: --

Rate limit:

Connections: --

Bandwidth: --

Inbound bandwidth: --

Outbound bandwidth: --

Connection synchronization: Enabled

Sticky synchronization: Disabled

Bandwidth busy protection: Disabled

Interface bandwidth statistics: Disabled

Route advertisement: Disabled