FGSP 配置指导

版本	V1.2
时间	2021 年 8 月
作者	王祥
状态	已审核
反馈	support_cn@fortinet.com

目录

1. 应用场景

FortiGate Session Life Support Protocol (FGSP)在异步流量负载分担的场景中实现单机会话同步，通常配合单机配置同步功能 Standalone Config Sync 一同使用，本文档示例中包含 FGSP 和单机配置同步的配置内容。

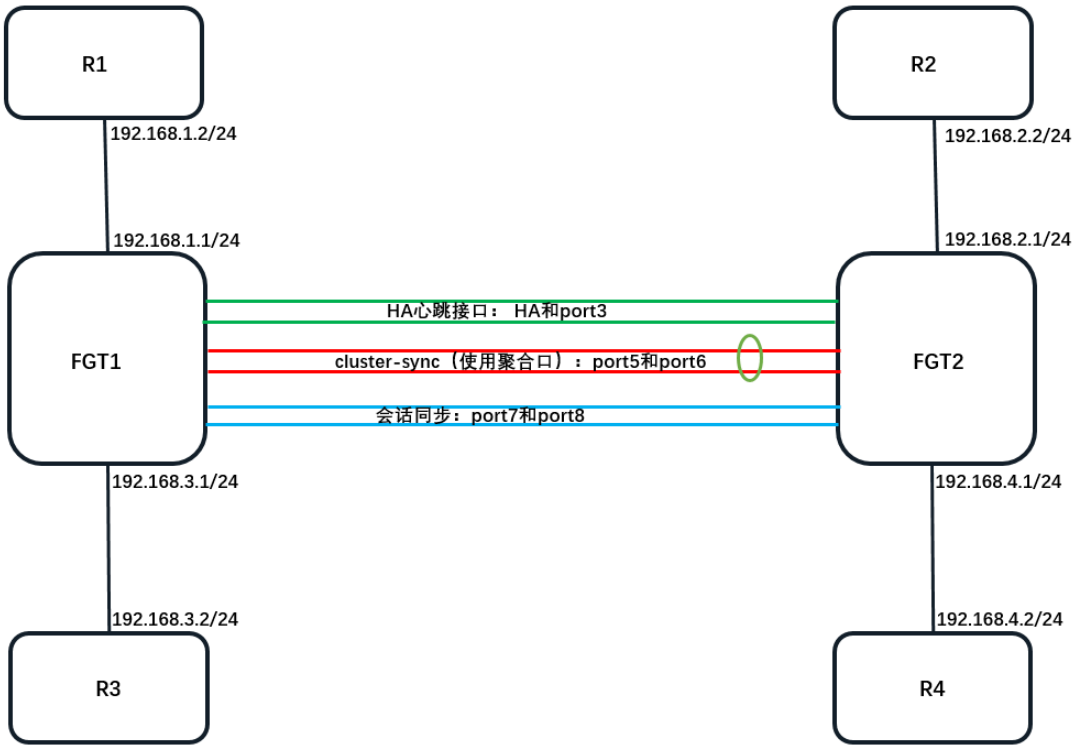
FGT v6.4 版本之前，如 v6.0，v6.2 FGSP 不支持 UTM/NGFW，v6.4 后开始支持，不同版本的配置和应用场景见后叙述。

2. 设备版本

FortiGate v6.4.6, build1879

3. FGSP 配置

3.1. 三层互联场景



3.2. 配置步骤

开启会话同步

```
config system ha
    #使能 cpu 负载分担会话同步，否则只有一个 cpu core 处理
    set sync-packet-balance enable
    #开启会话同步
    set session-pickup enable
    set session-pickup-connectionless enable
    set override disable
    #FGT1 配置为 200，FGT2 配置为 100
    set priority 200
end
```

配置 FGSP 组，选择 NP 加速接口作为会话同步的接口，如果设备有多个 NP 加速芯片，请选择不同 NP 加速芯片上的接口，并且配置巨帧避免数据包分片

```
config system interface
    edit "port7"
        set vdom "root"
        set mtu-override enable
        set mtu 9216
    next
    edit "port8"
        set vdom "root"
        set mtu-override enable
        set mtu 9216
    next
end

config system standalone-cluster
    # FGSP 集群 ID，每个 FGSP 集群 ID 必须一致
    set standalone-group-id 100
    #会话同步接口，使用二层报文传输
    set session-sync-dev "port7" "port8"
    #FGSP 成员 ID，标识 UTM 会话的所属者，即 HA_ID，FGSP 每个成员必须配置不一样的 ID，取值 0-15
    set group-member-id 5
end
```

cluster-sync 有两个默认选项（保持默认即可，不需要修改）：

peervd 默认使用 root vdom 的接口同步会话，peer-ip 接口所属的 vdom 要和 peervd 配置的 vdom 一样。

syncvd 表示哪些 vdom 的会话需要同步，默认为空，表示所有 vdom 的会话都同步。

cluster-sync 的配置有三个作用：

①指定会话同步的 vdom；

②作为 session-sync-dev 二层会话同步机制的备份，当 session-sync-dev 接口 down 时，使用 udp 报文进行会话同步；

③如果策略开启 UTM，将匹配该策略的流量重定向到“该会话的所有者”

选择 port5 和 port6 配置为聚合口作为 cluster-sync 的接口。由于 cluster-sync 接口目前只能配置一个，因此使用聚合接口来配置 peer-ip。选择 NP 加速接口作为会话同步的接口，如果设备有多个 NP 加速芯片，请选择不同 NP 加速芯片上的接口，并且配置巨帧避免数据包分片。

```
config system interface
    edit "peerbond"
        set vdom "root"
        set allowaccess ping
        set ip 10.1.1.1 255.255.255.0
        set type aggregate
        set member "port5" "port6"
        set mtu-override enable
        set mtu 9216
    next
end
config system cluster-sync //
     edit 1
        #peerip 指定对端设备 cluster-sync 接口的地址
        set peerip 10.1.1.2
    next
end
```

FGSP 如果有异步流量，请开启异步功能

```
config system settings
    set asymroute enable
end
```

开启配置同步（非必须，如果不开启可以手动配置）

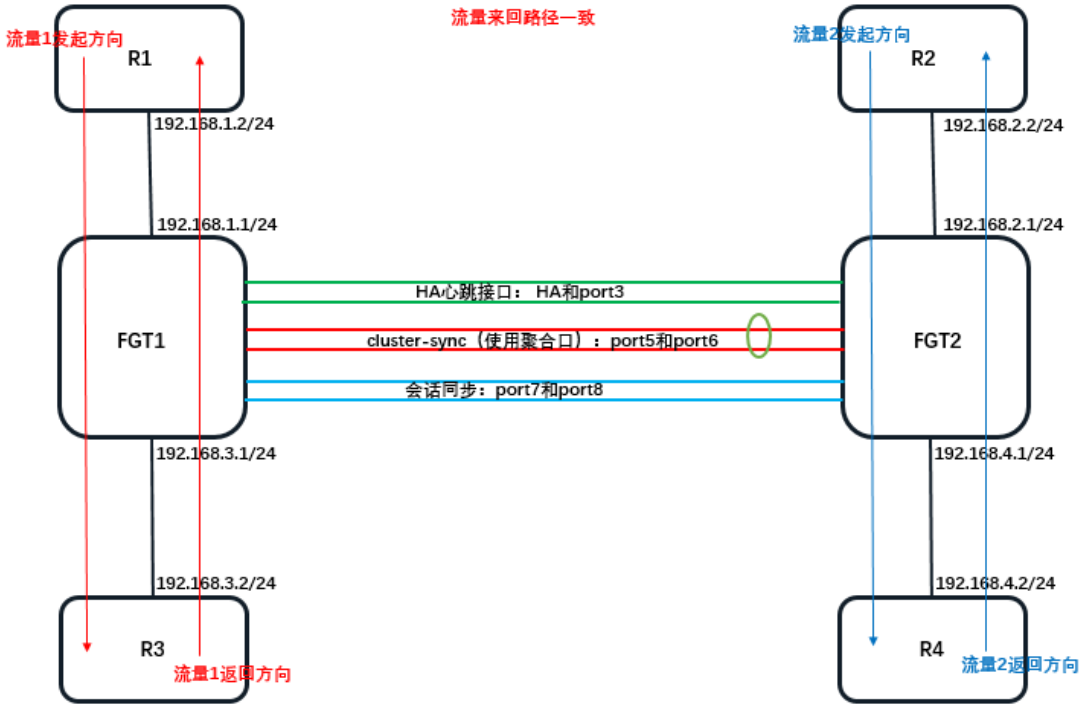
```
config system ha
    #配置同步接口，选择 NP port 和 CPU 直连接口，增加冗余
    set hbdev "ha" 0 "port3" 0
    #开启配置同步
    set standalone-config-sync enable
end
```

3.3. 数据流路径

①来回路径保持一致

流量发起方向：R1→FGT1→R3

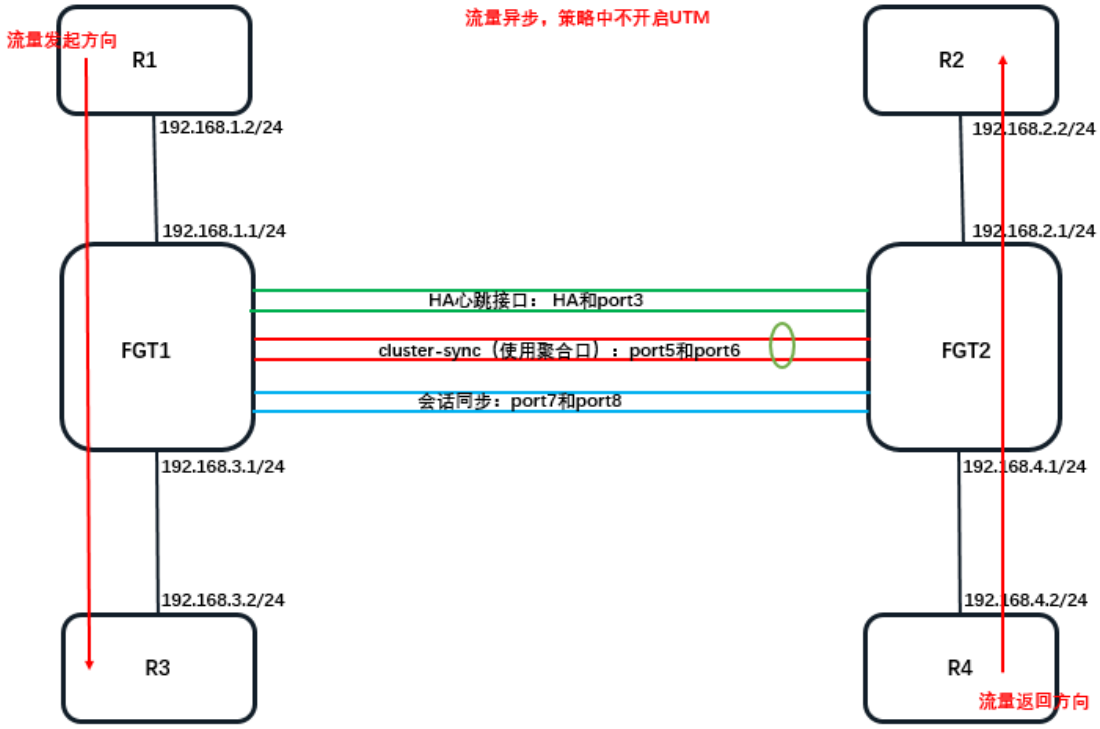
流量返回方向：R3→FGT1→R1



②有异步流量，策略不开启 UTM

流量发起方向：R1→FGT1→R3

流量返回方向：R4→FGT2→R2

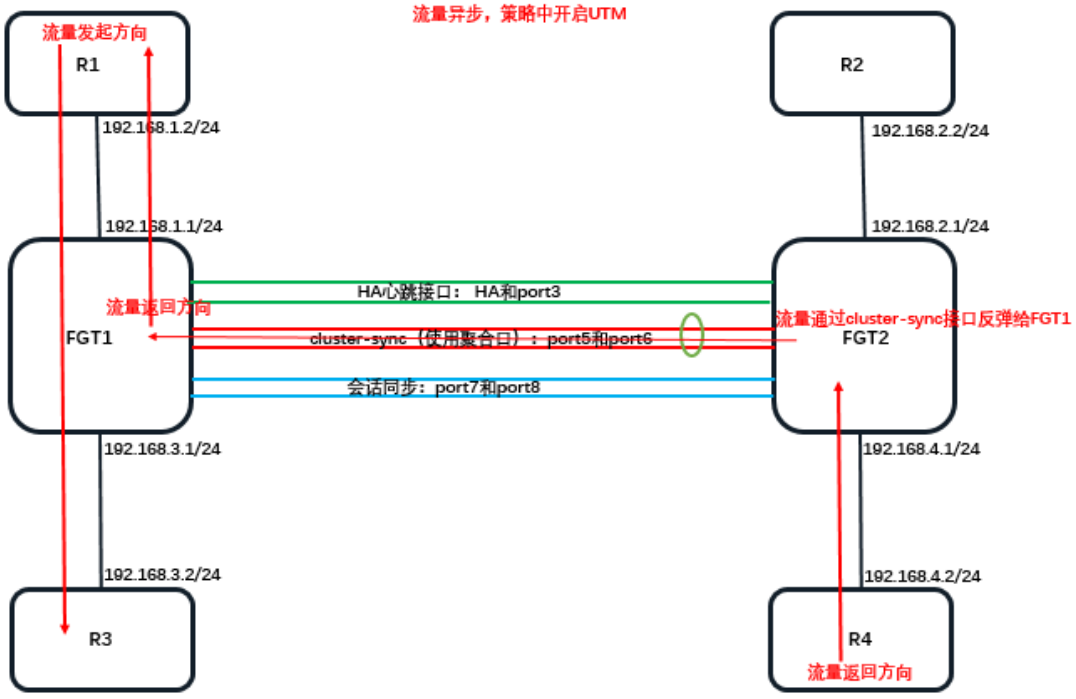


③有异步流量，策略中开启 UTM

流量发起方向：R1→FGT1→R3

流量返回方向：R4→FGT2(peer ip 接口)→FGT1→R1

与 UTM 相关的流量会通过 peer ip 接口弹回给 “该会话的所有者”，即收到第一个报文的设备。



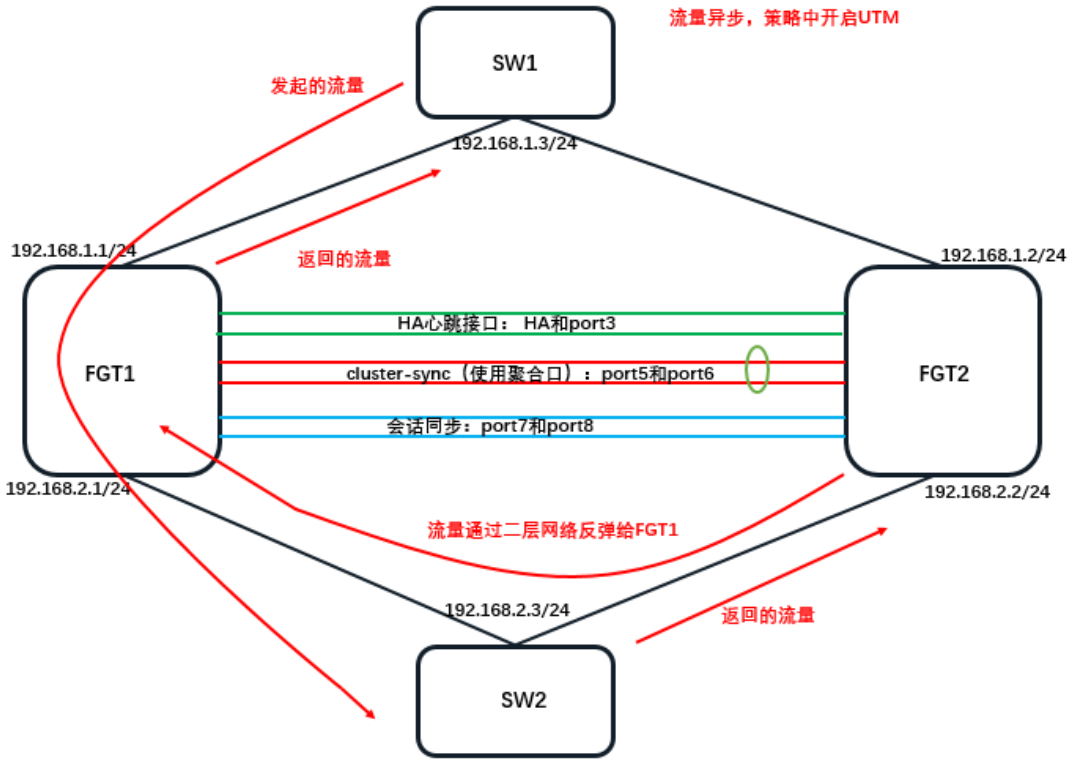
3. 4. 二层互联场景

如果 FGT1，FGT2 的上、下游设备都是二层互联。

3.2 章节的配置不变，可以增加如下配置。

```
config system standalone-cluster
    #FGSP 成员之间互联采用二层链路
    set layer2-connection available
end
```

策略开启 UTM 后，且 set layer2-connection available，FGSP 成员相同接口都在同一个网段，与 UTM 相关的流量会通过二层网络直接接口弹回给“该会话的所有者”，即收到第一个报文的设备。



4. FGT v6.4 之前版本的 FGSP 配置

4.1. 配置步骤

FGT v6.4 之前的版本，如 v6.0，v6.2 FGSP 不支持 UTM，也没有 config system standalone-cluster 配置命令。

拓扑如章节 3，三层互联场景和二层互联场景的配置是一样的。

开启二层会话同步

```
config system ha
    #使能 cpu 负载分担会话同步，否则只有一个 cpu core 处理
    set sync-packet-balance enable
    #开启会话同步
    set session-pickup enable
    set session-pickup-connectionless enable
    #会话同步接口，使用二层报文传输。选择 NP 加速接口作为会话同步的接口，如果设备有多个 NP 加速芯片，请选择不同 NP 加速芯片上的接口，并且配置巨帧避免数据包分片
    set session-sync-dev "port7" "port8"
    set override disable
    #FGT1 配置为 200，FGT2 配置为 100
    set priority 200
end
```

cluster-sync 有两个默认选项（保持默认即可，不需要修改）：

peervd 默认使用 root vdom 的接口同步会话，peer-ip 接口所属的 vdom 要和 peervd 配置的 vdom 一样。选择 NP 加速接口作为会话同步的接口，如果设备有多个 NP 加速芯片，请选择不同 NP 加速芯片上的接口，并且配置巨帧避免数据包分片。

syncvd 表示哪些 vdom 的会话需要同步，默认为空，表示所有 vdom 的会话都同步。

cluster-sync 的配置有两个作用：

①指定会话同步的 vdom；

②作为 session-sync-dev 二层会话同步机制的备份，当 session-sync-dev 接口 down 时，使用 udp 报文进行会话同步；

选择 port5 和 port6 配置为聚合口作为 cluster-sync 的接口。由于 cluster-sync 接口目前只能配置一个，因此使用聚合接口来配置 peer-ip。

```
config system interface
    edit "peerbond"
        set vdom "root"
        set allowaccess ping
        set ip 10.1.1.1 255.255.255.0
        set type aggregate
        set member "port5" "port6"
        set mtu-override enable
        set mtu 9216
    next
end
config system cluster-sync //
     edit 1
        #peerip 指定对端设备 cluster-sync 接口的地址
        set peerip 10.1.1.2
    next
end
```

FGSP 如果有异步流量，请开启异步功能。

```
config system settings
    set asymroute enable
end
```

开启配置同步（非必须，如果不开启可以手动配置）

```
config system ha
    #配置同步接口，选择 NP port 和 CPU 直连接口，增加冗余
    set hbdev "ha" 0 "port3" 0
    #开启配置同步
    set standalone-config-sync enable
end
```

5. 注意事项

① 形成 FGSP 的设备需要相同的型号和版本。

② FGTv6.4 之前的版本不支持 UTM。

③ 开启 standalone-config-sync enable 后，如果需要升级 FGT，则需要将 FGT 先从 FGSP 网络中分开，一台一台升级。不然如果直接升级，所有 FGT 会同步升级，将同时重启。配置恢复也是一样的。

④ 设备或者策略不支持 proxy 模式。

⑤ 重启 FGSP 环境中的设备时，如重启 FGT2，重启过程中，接口指示灯会在系统起来之前 UP，如果此时上下游就将流量送过来，系统不能处理，会引起短暂丢包。所以在组网时，与互联的设备之间配置动态路由或者上下游设备配置链路检测以避免此问题。

⑥ 由低版本升级到 V6.4 时，原有 HA 模块下 session-sync-dev 命令将移除，需要手动新增 config system standalone-cluster 下的配置来形成 FGSP。

⑦ FGTv6.4 或者之后的版本中，如果策略开启 UTM，匹配该策略的流量会通过 peer-ip 的接口反弹给“该会话的所有者”，如果 peer-ip 的接口发生故障 down 了，则匹配该策略的流量会中断。因此 peer-ip 所在的接口要使用聚合口，且聚合接口带宽要大于反弹的 UTM 流量。