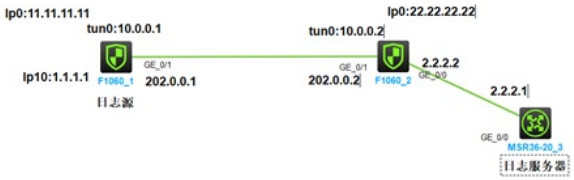
FW GRE OVER ISPEC发送快速日志典型配置

GRE VPN IPSec VPN Syslog日志 孔德飞 2022-07-16 发表

组网及说明

组网如下：

FW作为日志源，将安全策略日志以快速日志的方式发送到日志服务器，并且要保证发送日志被加密



配置步骤

主要配置如下：

FW1日志源主要配置

路由配置：

```
ip route-static 0.0.0.0 0 202.0.0.2
 ip route-static 2.2.2.0 24 Tunnel0
```

快速日志配置：

```
customlog format packet-filter
 customlog host 2.2.2.1 export packet-filter
 customlog host source LoopBack10
```

接口配置：

```
interface LoopBack0
 ip address 11.11.11.11 255.255.255.255
#
interface LoopBack10
 ip address 1.1.1.1 255.255.255.255
#

interface GigabitEthernet1/0/1
 port link-mode route
 combo enable copper
 ip address 202.0.0.1 255.255.255.0
 ipsec apply policy vpn
```

安全域与安全策略配置

```
security-zone name Trust
 import interface GigabitEthernet1/0/1
 import interface Tunnel0

security-policy ip（日志记录功能要打开）
 rule 0 name 0
  action pass
  logging enable
```

GRE主要配置

一定不要配置探测

```
interface Tunnel0 mode gre
 ip address 10.0.0.1 255.255.255.252
 source LoopBack0
 destination 22.22.22.22
 gre key 123
#
```

IPSSEC主要配置

```
acl advanced 3000
 rule 0 permit gre source 11.11.11.11 0 destination 22.22.22.22 0

ipsec transform-set tran1
 esp encryption-algorithm aes-cbc-256
 esp authentication-algorithm sha1
#
ipsec policy vpn 1 isakmp
 transform-set tran1
```

```
 security acl 3000
 remote-address 202.0.0.2
 ike-profile profile1
#
 ike identity fqdn vpn1
#
ike profile profile1
 keychain keychain1
 local-identity address 202.0.0.1
 match remote identity address 202.0.0.2 255.255.255.0
 proposal 1
#
ike proposal 1
 encryption-algorithm aes-cbc-256
 dh group2
#
ike keychain keychain1
 pre-shared-key address 202.0.0.2 255.255.255.255 key simple 123
```

FW2主要配置如下：

路由配置：

```
ip route-static 0.0.0.0 0 202.0.0.1
 ip route-static 1.1.1.0 24 Tunnel0
```

接口配置：

```
interface LoopBack0
 ip address 22.22.22.22 255.255.255.255
#
interface GigabitEthernet1/0/0
 port link-mode route
 combo enable copper
 ip address 2.2.2.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode route
 combo enable copper
 ip address 202.0.0.2 255.255.255.0
 ipsec apply policy vpn
```

安全域与安全策略配置

```
security-zone name Trust
 import interface GigabitEthernet1/0/0
 import interface GigabitEthernet1/0/1
 import interface Tunnel0

security-policy ip
 rule 0 name 0
  action pass
```

GRE主要配置

一定不要配置探测

```
interface Tunnel0 mode gre
 ip address 10.0.0.2 255.255.255.252
 source LoopBack0
 destination 11.11.11.11
 gre key 123
#
```

IPSSEC主要配置

```
acl advanced 3000
```

配置关键点

配置关键点

1. 配置快速日志的源目要走tunnel口
2. 快速日志必须以GRE OVER IPSEC的方式加密，因为快速日志如果以IPSEC加密方式发送，将不走安全策略业务点
3. 安全策略中将log enable打开
4. 安全策略日志模块为packet-filter

```
 rule 0 permit gre source 22.22.22.22 0 destination 11.11.11.11 0

ipsec transform-set tran1
 esp encryption-algorithm aes-cbc-256
 esp authentication-algorithm sha1
#
ipsec policy vpn 1 isakmp
```