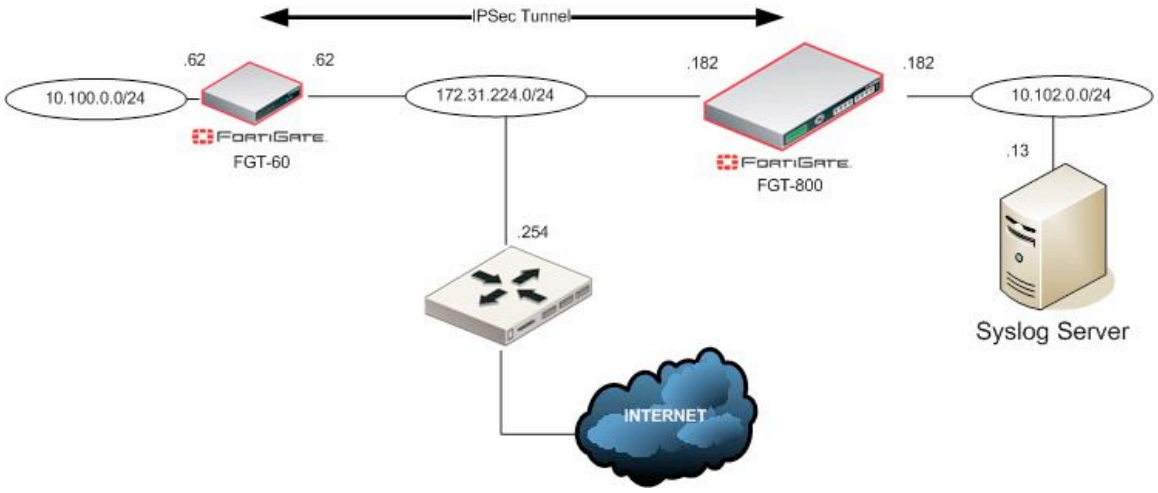
Sending Syslog files from a FortiGate over a Fortinet IPSec tunnel

This article concerns all FortiGate units running FortiOS 2.80.

In the setup below, the FortiGate-60 sends its generated syslogs to the Syslog server behind the FortiGat-800 in the head office. Internal users behind the FortiGate-60 will also be accessing resources behind the remote FortiGate-800, through an IPSec VPN. The following example also assumes that the FortiGate-60 uses a static public IP on its wan1 interface.



Configuration of the FortiGate 60

The first policy will allow the Syslog generated by the FortiGate-60 to be sent through the tunnel, to the remote Fortigate unit. The second policy will allow normal communication between the two private subnets over the tunnel. The third will allow regular internal traffic to access the Internet, unencrypted.

Firewall addresses

```
config firewall address
    edit "all"
    next
    edit "100"
        set subnet 10.100.0.0 255.255.255.0
    next
    edit "102"
        set subnet 10.102.0.0 255.255.255.0
    next
    edit "extern"
        set subnet 172.31.224.62 255.255.255.255
    next
    edit "syslogserver"
        set subnet 10.102.0.13 255.255.255.255
    next
end
```

IPSec configuration

```
config vpn ipsec phase1
    edit "Ph1-102"
        set dpd enable
        set nattraversal enable
        set proposal 3des-md5
        set mode aggressive
        set remotegw 172.31.224.182
 set psksecret ENC M6ZRe2tQhCBk0wMjCTTyni1
    next
end
config vpn ipsec phase2
    edit "Ph2-102"
        set dhgrp 1
        set keepalive enable
        set phase1name "Ph1-102"
    next
end
```

Firewall Policies

```
config firewall policy
    edit 1
        set srcintf "internal"
        set dstintf "wan1"
        set srcaddr "extern"
        set dstaddr "syslogserver"
        set action encrypt
        set schedule "always"
        set service "SYSLOG"
        set logtraffic enable
        set inbound enable
        set outbound enable
        set vpntunnel "Ph2-102"
    next
    edit 2
        set srcintf "internal"
        set dstintf "wan1"
        set srcaddr "100"
        set dstaddr "102"
        set action encrypt
        set schedule "always"
        set service "ANY"
        set logtraffic enable
        set inbound enable
        set outbound enable
        set vpntunnel "Ph2-102"
    next
    edit 3
        set srcintf "internal"
        set dstintf "wan1"
        set srcaddr "100"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ANY"
        set logtraffic enable
        set nat enable
    next
end
```

Syslog configuration

```
config log syslogd setting
    set server "10.102.0.13"
    set status enable
```

```
end
```

Configuration of the FortiGate 800

Firewall addresses

```
config firewall address
    edit "all"
    next
    edit "100"
        set subnet 10.100.0.0 255.255.255.0
    next
    edit "102"
        set subnet 10.102.0.0 255.255.255.0
    next
    edit "syslogserver"
        set subnet 10.102.0.13 255.255.255.255
    next
    edit "fgt60-2"
        set subnet 172.31.224.62 255.255.255.255
    next
end
```

IPSec configuration

```
config vpn ipsec phase1
    edit "Ph1-100"
        set dpd enable
        set nattraversal enable
        set proposal 3des-md5
        set mode aggressive
        set remotegw 172.31.224.62
        set psksecret ENC 9aDxT+luep1d+dR1iOUXnOZPJDN
    next
end
config vpn ipsec phase2
    edit "Ph2-100"
        set dhgrp 1
        set keepalive enable
        set phase1name "Ph1-100"
    next
end
```

Firewall Policies

```
config firewall policy
    edit 1
        set srcintf "internal"
        set dstintf "external"
        set srcaddr "syslogserver"
        set dstaddr "fgt60-2"
        set action encrypt
        set schedule "always"
        set service "ANY"
        set logtraffic enable
        set inbound enable
        set outbound enable
        set vpntunnel "Ph2-100"
    next
    edit 3
        set srcintf "internal"
        set dstintf "external"
        set srcaddr "102"
        set dstaddr "100"
        set action encrypt
        set schedule "always"
        set service "ANY"
```

```
        set logtraffic enable
        set inbound enable
        set outbound enable
        set vpntunnel "Ph2-100"
    next
    edit 4
        set srcintf "internal"
        set dstintf "external"
        set srcaddr "102"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ANY"
        set logtraffic enable
        set nat enable
    next
end
```