

## pfSense - Bug #10517

### Mobile PSK user mobile-userpool is ignored

05/01/2020 06:13 AM - Viktor Gurov

<b>Status:</b>	Not a Bug	<b>Start date:</b>	05/01/2020
<b>Priority:</b>	Normal	<b>Due date:</b>	
<b>Assignee:</b>	Jim Pingle	<b>% Done:</b>	0%
<b>Category:</b>	IPsec	<b>Estimated time:</b>	0.00 hour
<b>Target version:</b>	2.5.0	<b>Affected Architecture:</b>	
<b>Affected Version:</b>	2.5.0		

#### Description

regardless of what you entered in the "Virtual Address Pool" on the VPN / IPsec / Pre-Shared Keys / Edit page, mobile clients will always receive an IP address from "Virtual Address Pool" of "Mobile Clients".

sample config:

```
# This file is automatically generated. Do not edit
connections {
    bypass {
        remote_addrs = 127.0.0.1
        children {
            bypass {
                local_ts = 192.168.3.0/24,fcaa:10:1:1::/64
                remote_ts = 192.168.3.0/24,fcaa:10:1:1::/64
                mode = pass
                start_action = trap
            }
        }
    }
}
con-mobile : con-mobile-defaults {
    # Stub to load con-mobile-defaults
}
con-mobile-userpool-1 : con-mobile-defaults {
    remote {
        id = userfqdn:test1
        eap_id = %any
    }
    pools = mobile-userpool-1
}
con-mobile-userpool-2 : con-mobile-defaults {
    remote {
        id = userfqdn:test3
        eap_id = %any
    }
    pools = mobile-userpool-2
}
}
con-mobile-defaults {
    fragmentation = yes
    unique = replace
    version = 2
    proposals = aes128-sha256-modp2048
    dpd_delay = 10s
    dpd_timeout = 60s
    reauth_time = 28800s
    rekey_time = 0s
    encap = no
    mobike = no
    local_addrs = 192.168.3.4
```

```

remote_addrs = 0.0.0.0/0,::/0
pools = mobile-pool-v4
send_cert = always
local {
    id = 192.168.3.4
    auth = pubkey
    cert {
        file = /var/etc/ipsec/x509/cert-1.crt
    }
}
remote {
    eap_id = %any
    auth = eap-mschapv2
}
children {
    con-mobile {
        dpd_action = clear
        mode = tunnel
        policies = yes
        life_time = 3600
        start_action = none
        local_ts = 172.16.16.0/30
        esp_proposals = aes128-sha256-modp2048,aes128gcm128-modp2048
    }
}
}
pools {
    mobile-pool-v4 : mobile-pool {
        addrs = 10.33.33.0/24
    }
    mobile-userpool-1 : mobile-pool {
        addrs = 10.11.11.1/32
    }
    mobile-userpool-2 : mobile-pool {
        addrs = 10.34.34.5/24
    }
}
secrets {
    private-0 {
        file = /var/etc/ipsec/private/cert-1.key
    }
    eap-1 {
        secret = 0sMTIz
        id-0 = test1
    }
    ike-2 {
        secret = 0sMTIz
        id-0 = test2
    }
    eap-3 {
        secret = 0sMTIz
        id-0 = test3
    }
}
}

```

test1-3 users always get IP from 10.33.33.0/24

pfSense 2.5.0.a.20200430.1700

## History

#1 - 05/01/2020 07:20 AM - Jim Pingle

- Assignee set to Jim Pingle

- Target version set to 2.5.0

This was working not long ago, something else must have broken it again.

## #2 - 05/01/2020 08:31 AM - Jim Pingle

- Status changed from New to Not a Bug

I'm not seeing a problem here.

```
con-mobile-userpool-1 : con-mobile-defaults {
  remote {
    id = "eapuser1"
    eap_id = %any
  }
  pools = mobile-userpool-1
}
```

```
pools {
  mobile-pool-v4 : mobile-pool {
    addrs = 10.6.240.0/24
    subnet = 10.6.0.0/24
    split_include = 10.6.0.0/24
  }
  mobile-pool-v6 : mobile-pool {
    addrs = 2001:db8:1:ef09::/64
    subnet = 2001:db8:1:ee70::/64
    split_include = 2001:db8:1:ee70::/64
  }
  mobile-userpool-1 : mobile-pool {
    addrs = 10.6.211.0/24
    dns = 8.8.8.8
  }
  mobile-userpool-2 : mobile-pool {
    addrs = 10.6.95.0/24
    dns = 1.1.1.1
  }
}
mobile-pool {
  dns = 10.6.0.1,198.51.100.1,8.8.8.8,8.8.4.4
  nbns = 172.21.32.2
  # Search domain and default domain
  28672 = "Welcome"
}
```

```
secrets {
  eap-7 {
    secret = 0sZWFwdXNlcjE=
    id-0 = eapuser1
  }
}
```

```
: swanctl --list-pools --leases
mobile-pool-v4      10.6.240.0          0 / 0 / 254
mobile-userpool-2  10.6.95.0          0 / 0 / 254
mobile-userpool-1  10.6.211.0        1 / 0 / 254
  10.6.211.1          online   'eapuser1'
mobile-pool-v6      2001:db8:1:ef09:: 0 / 0 / 2147483646
```

There is no identifier type selected on my user, and yours is set to userfqdn. Maybe your client isn't sending it as the proper type. The config is correct.

**#3 - 05/01/2020 08:59 AM - Viktor Gurov**

hm, this is strongswan-nm 5.7.2-1 on Debian 10

**#4 - 05/01/2020 09:02 AM - Jim Pingle**

And I'm using the strongSwan app (v 2.2.1) on Android.

Is the ID actually configured as userfqdn in the client?