aahmadzada
Staff

Created on
10-06-2022 04:48 AM

Article Id
205919

Technical Tip: FortiGate configured with multiple captive portals and as a DNS server

Description

This article covers the configuration of two DNS servers along with the captive portal on two different interfaces of FortiGate.

Scope

FortiOS 7.0.6 and newer versions.

Solution

On FortiOS versions prior to 7.0.6, it was possible to configure auth-portal-addr globally:

```
# config firewall auth-portal
    set portal-addr "fgt.test.lab"
end
```

That was creating problems for some users, who wanted to implement a captive portal on more than one interface.

For instance, the captive portal is deployed on port2 and port3.

IP address of port2 is 192.168.100.1
IP address of port3 is 192.168.200.1

The authentication portal address is configured like this:

```
# config firewall auth-portal
    set portal-addr "fgt.test.lab" 3
end
```

Client connected to port2 will hit the captive portal and will be redirected to fgt.test.lab, which has to be resolved as the IP address of the port2.
Client connected to port3 will hit the captive portal and will be redirected to fgt.test.lab, which has to be resolved as the IP address of the port3.

So there should be a DNS solution, that will resolve the fgt.test.lab as one of the IP addresses of the interfaces (IP address of port2 or port3).

If the DNS request to resolve fgt.test.lab comes from port2, the fgt.test.lab has to be resolved as an ip address of port2 (192.168.100.1), so the client can reach the captive portal, which is running on port2.

If the DNS request to resolve fgt.test.lab comes from port3, the fgt.test.lab has to be resolved as an ip address of port3 (192.168.200.1), so the client can reach the captive portal, which is running on port3.

Prior to FortiOS 7.0.6, in such scenarios, the user had to deploy micro DNS servers on each port, which is configured as the captive portal.

The DHCP server assigns DNS server 1 for the clients connected to port2.
The DHCP server assigns DNS server 2 for the clients connected to port3.

As a result:

DNS Server 1 should resolve fgt.test.lab as 192.168.100.1.
DNS Server 2 should resolve fgt.test.lab as 192.168.200.1.

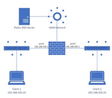
By doing so, each captive portal client will be able to resolve the fgt.test.lab to the appropriate IP address of FortiGate.

Starting from FortiOS 7.0.6, an improvement was implemented so the addresses for the authentication portal can also be configured under the interface(s), which are configured as a captive portal.

```
    edit "port2"
        set vdom "root"
        set ip 192.168.100.1 255.255.255.0
        set allowaccess ping https http
        set type physical
        set security-mode captive-portal
        set auth-portal-addr "fgt.captivel.test.lab" 3
        set snmp-index 2
    next
```

In such a case, the FortiGate can also be configured as a DNS server that will resolve the address of the auth-portal-addr.

This document will cover the scenario where port2 and port3 are configured as a captive portal and additionally the FortiGate is running as the DNS server.



1) Configure Interfaces on FortiGate:

```
# config system interface
    edit "port1"
        set vdom "root"
        set ip 192.168.180.101 255.255.255.0
        set allowaccess ping https ssh http telnet
        set type physical
        set snmp-index 1
    next
    edit "port2"
        set vdom "root"
        set ip 192.168.100.1 255.255.255.0
        set allowaccess ping https http
        set type physical
        set security-mode captive-portal
        set auth-portal-addr "fgt.captivel.test.lab" 3
        set snmp-index 2
    next
    edit "port3"
        set vdom "root"
        set ip 192.168.200.1 255.255.255.0
        set allowaccess ping https http
        set type physical
        set security-mode captive-portal
        set auth-portal-addr "fgt.captive2.test.lab"3
        set role lan
        set snmp-index 3
    next
```

2) Configure the default route on FortiGate:

```
# config router static
    edit 1
        set gateway 192.168.180.2
        set device "port1"
    next
end
```

3) Configure firewall policies for each port:

```
# config firewall policy
    edit 1
        set name "captive_port2"
        set srcintf "port2"
        set dstintf "port1"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set nat enable
    next
    edit 2
        set name "captive_port3"
        set srcintf "port3"
        set dstintf "port1"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end
```

4) Configure DNS Server on FortiGate:

```
# config system dns-server
    edit "port2"
    next
    edit "port3"
    next
end

# config system dns-database
    edit "zone1"
        set domain "test.lab"

# config dns-entry
    edit 1
        set hostname "fgt.captivel.test.lab" 3 auth-portal-addr configured for port2
        set ip 192.168.100.1
    next
    edit 2
        set hostname "fgt.captive2.test.lab" 3 auth-portal-addr configured for port3
        set ip 192.168.200.1
    next
end
    next
end
```

5) Configure DHCP pools on FortiGate:

```
# config system dhcp server
    edit 2
        set default-gateway 192.168.100.1
        set netmask 255.255.255.0
        set interface "port2"

# config ip-range
    edit 1
        set start-ip 192.168.100.10
        set end-ip 192.168.100.200
    next
end
        set timezone-option default
        set dns-server1 192.168.100.1
    next
    edit 3
        set default-gateway 192.168.200.1
        set netmask 255.255.255.0
        set interface "port3"

# config ip-range
    edit 1
        set start-ip 192.168.200.10
        set end-ip 192.168.200.200
    next
end
        set timezone-option default
        set dns-server1 192.168.200.1
    next
end
```

6) Results on client PC connected to port2:

7) Results on client pc connected to port3: