Using Port 443 for MGMT Access and SSL VPN

Scope:

- Accessing the FortiGate's management page and SSL VPN on TCP port 443
- By default this is not possible as port 443 can only be assigned to one system service.
- Since SSL VPN and HTTPS administrative access are two different system services a workaround is required.

Requirements:

- Two publicly routable IP addresses (One additional to the one assigned on the outside interface)
- Space to create a loopback interface (There is a 128-256 max object limit for interfaces)
- Space to create a VIP (max VIP objects may be applicable)
- Space to create a firewall address object (max address objects may be applicable)
- Completed configuration of SSL VPN portal and settings
- Completed configuration of user groups to be used for SSL VPN authentication

  Note: For a list of max values please visit the link below:
  http://docs-legacy.fortinet.com/fgt/handbook/40mr3/fortigate-max-values-40-mr3.pdf

Step-by-step instructions:

1. Assign the additional external IP address to the outside interface by navigating to:
   a. System > Network > Interface
   b. Edit the external interface
   c. Check "Secondary IP Address"
   d. Click "Add"
   e. Enter the IP address with subnet mask and choose desired administrative access (As this will only be used for SSL VPN it is recommended to leave all services unchecked).
   f. Hit OK
   g. Hit OK

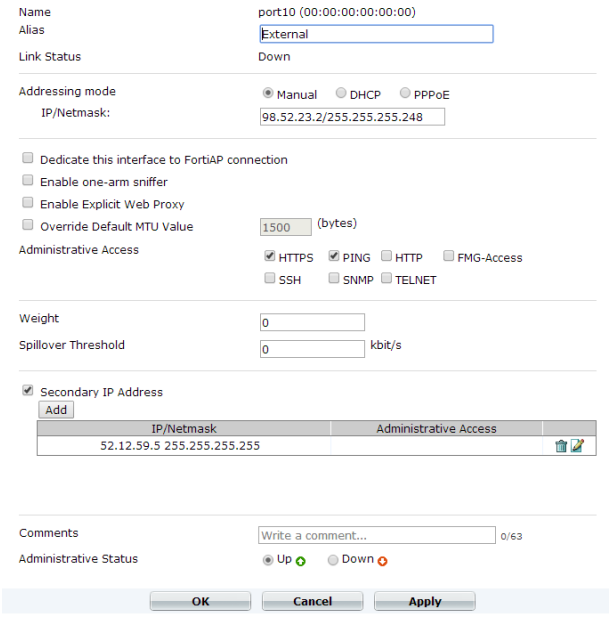

Figure 1: Secondary IP Address on External Interface

2. Create a loopback interface

a. Navigate to System > Network > Interface
b. Click on "Create New"
c. Name the interface (i.e.: SSLVPN_Loopback)
d. Choose Type "Loopback Interface"
e. Enter any unused IP address (Leave all Administrative Access services unchecked)
f. Hit OK

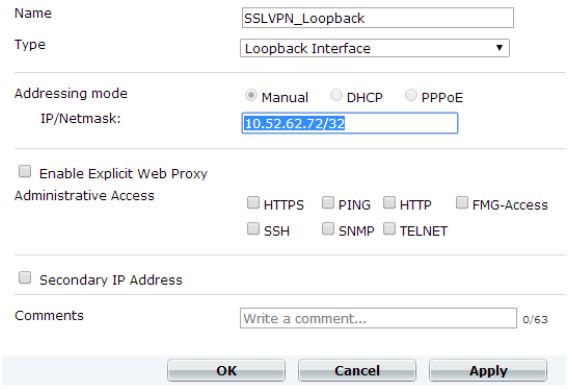

Figure 2: Loopback Interface

3. **Create a Virtual IP (NAT)**
    a. Navigate to Firewall Objects > Virtual IP > Virtual IP
    b. Click "Create New"
    c. Name the object (i.e.: SSLVPN_VIP)
    d. Choose your external interface
    e. Enter your secondary external IP in the "External IP Address/Range" field
    f. Enter your loopback interface's IP in the "Mapped IP Address/Range" field
    g. Check "Port Forwarding"
    h. Enter 443 in the "External Service Port" field
    i. Enter 10443 in the "Map to Port" field

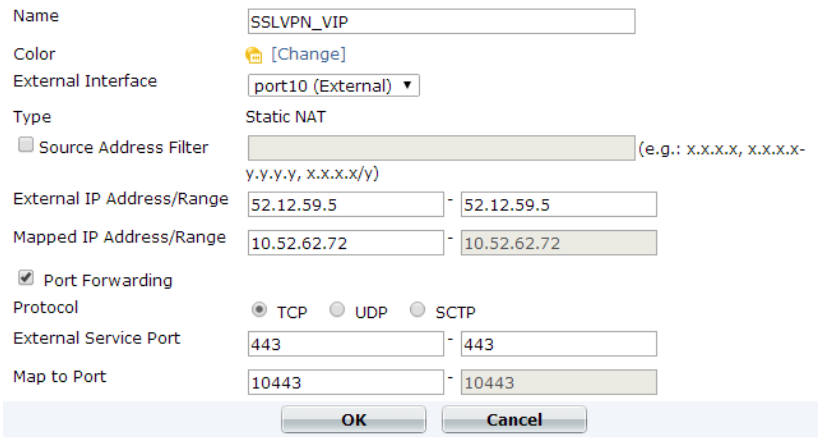

Figure 3: VIP - Translate SSLVPN traffic from port 443 to 10443

4. **Configure firewall policy with VIP**
    a. Navigate to Policy > Policy > Policy
    b. Click "Create New"
    c. Choose your external interface as the source interface
    d. Choose the loopback interface as the destination interface
    e. Choose "all" as the source address
    f. Choose the newly created VIP as the destination address
    g. Choose "ANY" for the Service
    h. Leave all other settings at default
    i. Hit OK

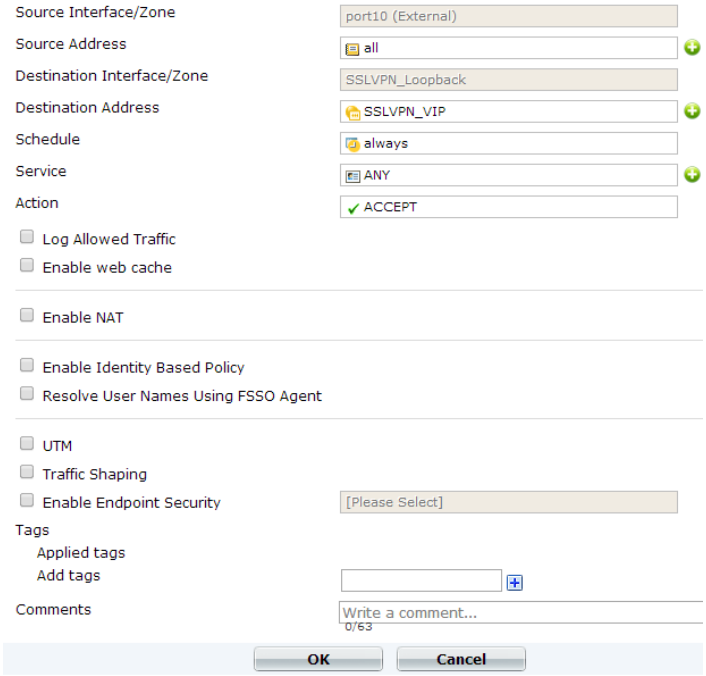

Figure 4: Loopback/VIP Firewall Policy

5. **Configure all necessary SSL VPN firewall policies.**
   This part is described and explained in detail in the SSL VPN documentation: http://docs-legacy.fortinet.com/fgt/handbook/40mr3/fortigate-sslvpn-40-mr3.pdf

   The difference here is that instead of using the external interface we configure all our policies using the Loopback interface.

   In order to configure the main SSL VPN authentication policy follow these steps:
   a. Go to Policy > Policy > Poliy
   b. Choose your Loopback interface for source interface
   c. Choose your internal interface for destination interface or whichever network you would like to provide access to via SSL VPN.
   d. Choose "all" for source address
   e. Choose your internal network for destination address (This might have to be configured if it has never been created)
   f. Choose "SSL-VPN" for Action
   g. Click on "Add" to add the user group which is allowed to authentication against the SSL VPN
   h. Select the appropriate options for Service and Schedule (ANY and ALWAYS in this example)
   i. Hit OK

j. Hit OK

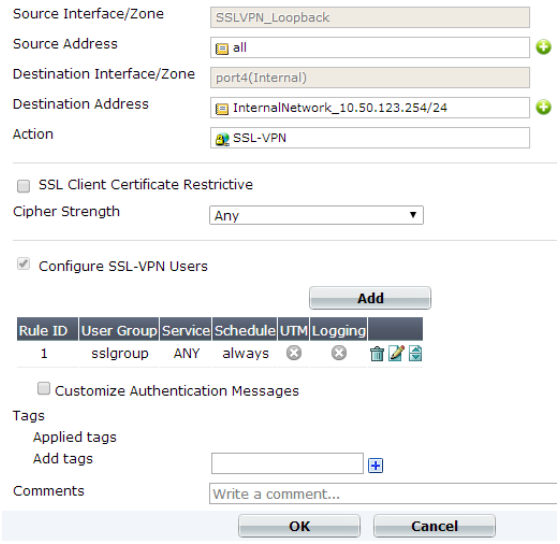

Figure 5: SSL VPN Authentication Firewall Policy

6. **Access both IPs on port 443**

   You should now be able to access your primary external IP on port 443 and be presented with the FortiGate administrator logon screen. Likewise, you should also be able to access the secondary external IP on port 443 and be presented with the SSL VPN logon screen.

   Note that you will not be able to access the SSL VPN via the primary IP address on port 10443 unless you configure the same firewall policy as in step 5, exchanging the loopback interface for the external interface.