Integrating Fortinet into an OSPF Network

Version	1.0
Date	10/11/04
Product	FortiOS 2.8
Description	This technical note describes the configuration steps necessary to integrate Fortinet into an OSPF network.
Author	Jason Clark

Send comments regarding this document to jclark@fortinet.com

Contents

Introduction

OSPF is a link state routing protocol based on the SPF (shortest path first) algorithm. Hence each router maintains a link state database which defines the topology of the Autonomous System. An autonomous system is comprised of a group of areas connected to a backbone.

Fortinet can participate within OSPF areas, as well as act as an ABR or ASBR. There are four required configuration steps in order to enable OSPF support within a Fortigate platform. This document covers these four requirements; router id, area, network, and interfaces. We will also touch on some best practices for securing OSPF.

This technical note assumes a basic understanding of the OSPF protocol. For additional OSPF information please review RFC 2328.

Configuration

There are a number of configurable OSPF options within FortiOS 2.8. OSPF settings are currently configurable via the FortiOS command line interface. This section covers the required configurable parameters for enabling OSPF. The four parameters discussed are as follows:

- **Router ID**
- **Area**
- **Network**
- **OSPF Interface**

Router ID

By default Fortinet does not create a Router ID value. Thus, this must be manually configured. The Router ID should be a 32-bit number that uniquely identifies a participating router with a routing domain or Autonomous System. A Router ID of 0.0.0.0 is not allowed as this value is used during the designated router and BDR elections.

Perform the following steps to configure the router id

Enter OSPF router configuration mode

```
configure router ospf <enter>
```

From the ospf# prompt, set the 32-bit router id.

```
set router-id "ip address" <enter>
```

Type "end" to save changes

Example

```
configure router ospf
  set router-id 192.168.1.99
            end
```

AREA

Routing devices in an OSPF Autonomous System are organized into groupings referred to as areas. All routers within an area maintain link state databases for their specific area. An area id of 0 or 0.0.0.0 indicates the backbone area. There must be a backbone for which areas can connect to. Virtual links can be used for areas that do not have a connection to the backbone. A maximum of 20 areas is allowed across all models.

Perform the following steps to specify the area for with the Fortigate will participate in.

Enter OSPF router configuration mode

```
configure router ospf <enter>
```

From the ospf# prompt enter the area sub menu

```
configure area <enter>
```

From the area# prompt create the area ID

```
edit "area ID" <enter>
```

Type "end" to save changes

Example

```
configure router ospf
      configure area
            edit 0.0.0.0
            end
```

Note: Within the area menu, you have the option to configure additional parameters such as area type, authentication, and filtering. Some of these optional parameters will be covered later in this document.

Network

Within a Fortigate the network command specifies networks and interfaces belonging to an Area. Multiple networks can be assigned to a single physical network. A maximum of 100 networks is allowed is across all models.

Perform the following steps assign a network interface(s) to an area.

Enter OSPF router configuration mode

```
configure router ospf <enter>
```

Enter the network configuration submenu

```
configure network <enter>
```

Create a network entry ID in the form of an integer

```
edit "integer" <enter>
```

Create subnet/supernet

```
set prefix "IP" "Subnet Mask" <enter>
```

Attach network to specific area.

```
set area "area_id" <enter>
```

Type “end” to save changes.

Note: Multiple networks can be defined by creating additional ID Integers.

OSPF Interface

To apply your OSPF configuration, you must specify an interface name, IP address, as well as a physical interface. Within the OSPF interface configuration you also have the ability to configure additional parameters that will help determine link state information. Such parameters include cost, priority, and status, among others. Descriptions of these optional parameters can be found in the Fortigate 2.8 CLI reference guide.

Perform the following steps to apply an OSPF configuration to a specific interface(s)

Enter OSPF router configuration mode

```
configure router ospf <enter>
```

Enter interface configuration mode

```
configure ospf-interface <enter>
```

Create a descriptive interface name

```
edit “interface name” <enter>
```

Specify a physical interface

```
set interface “interface name” <enter>
```

Note: Interface_name must be a configured physical interface

Type “end” to save changes.

Example

```
configure router ospf
      configure ospf-interface
          edit internal
          set interface internal
              end
```

Validation

FortiOS offers various commands to validate and verify OSPF configuration. We will cover multiple verification options.

To validate that OSPF is enabled on a specific interface we will use the following command

```
get router info ospf interface <enter>
```

The output should be as follows

```
wan2 is down, line protocol is down
  OSPF not enabled on this interface
wan1 is up, line protocol is up
  OSPF not enabled on this interface
dmz is up, line protocol is up
  OSPF not enabled on this interface
internal is up, line protocol is up
   Internet Address 192.168.1.99/24, Area 0.0.0.0, MTU 1500
     Router ID 192.168.1.99, Network Type BROADCAST, Cost:
   10
    Transmit Delay is 1 sec, State DR, Priority 1
      Designated Router (ID) 192.168.1.99, Interface
Address 192.168.1.99
    No backup designated router on this network
      Timer intervals configured, Hello 10, Dead 40, Wait
40, Retransmit 5
    Hello due in 00:00:08
Neighbor Count is 1, Adjacent neighbor count is 1
    Crypt Sequence Number is 0
Hello received 81 sent 81, DD received 8 sent 3
S-Req received 0 sent 3, LS-Upd received 4 sent 2
LS-Ack received 2 sent 3, Discarded 0
root is up, line protocol is up
  OSPF not enabled on this interface
ppp0 is up, line protocol is up
  OSPF not enabled on this interface
```

The above output tells us that OSPF is enabled on the internal interface and this device is acting as the Designated Router. We also see that our adjacent neighbor count is 1.

To view our OSPF neighbors use the following command

```
get router info ospf neighbor <enter>
```

The output should be as follows

```
Neighbor ID  Pri State Dead Time Address      Interface
192.168.1.32 0   Full  00:00:38  192.168.1.32 internal
```

To view the current OSPF routing entries use the following

```
get router info ospf route <enter>
```

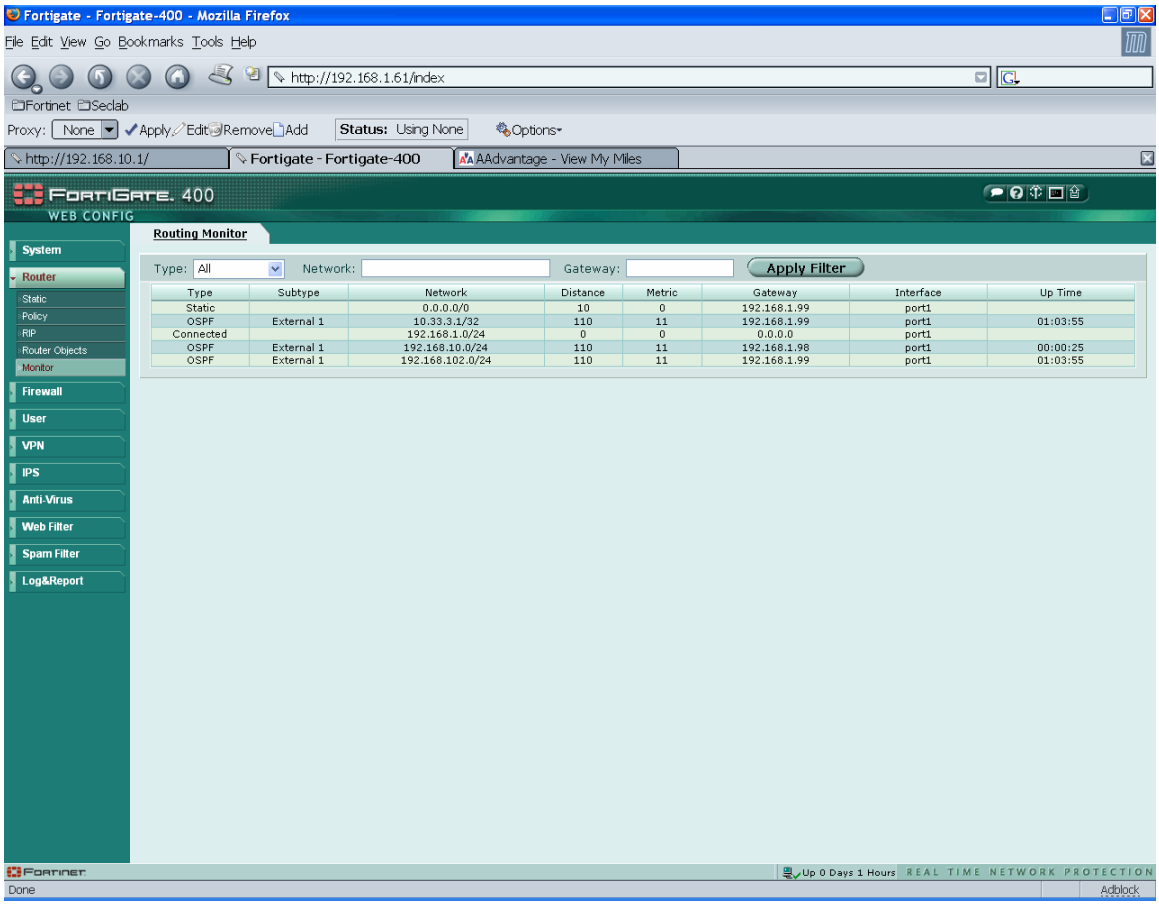
The output should be as follows

```
OSPF process 1:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF
inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA
external type 2 E1 - OSPF external type 1, E2 - OSPF
external type 2

E1 0.0.0.0/0 [12] via 192.168.1.99, port1
E1 10.33.3.1/32 [11] via 192.168.1.99, port1
O  192.168.1.0/24 [10] is directly connected, port1, area 0
```

```
E1 192.168.102.0/24 [11] via 192.168.1.99, port1
```

The OSPF routing table may also be viewed from the Web UI as shown below



System Resources

There are two main system resource factors to keep in mind when implementing a Fortigate into your OSPF network. The first is memory as OSPF utilizes system memory to store routing information. The size of an OSPF LSA is a minimum of 32 bytes, although is typically around 64 bytes.

The second resource factor is CPU utilization. The SPF algorithm uses CPU cycles to generate routing entries when link state changes. By default a Fortigate will perform an SPF calculation 5 seconds after receiving new routing information.

When integrating a Fortigate into an OSPF network proper sizing is critical as FortiOS utilizes memory and CPU for additional functions. Additional parameters can be tuned to ensure optimum resource utilization. Some of these parameters will be covered below.

SPF Timers

Fortinet allows for the configuration of SPF delay time and SPF hold time as discussed below.

The SPF delay_integer specifies the delay after a routing update is received until the SPF calculation is performed. The SPF hold_integer specifies the time between SPF calculations. The default in seconds is 5 for the delay_integer and 10 for the hold_integer.

If the OSPF routing environment permits, you can increase the delay and frequency in which SPF calculations are performed.

To adjust these values, perform the following

Enter OSPF router configuration mode

```
configure router ospf <enter>
```

Configure values where the first number is the delay integer and the second is the hold integer

```
set spf-timers "delay_integer" "hold_integer" <enter>
```

Example

```
configure router ospf
    set spf-timers 60 3600
    end
```

Database Overflow

Database overflow configuration can provide relief from unnecessary or sudden flooding of LSA's. While database overflow state cannot validate the quality of an LSA it can limit the database usage. Additional information on the database overflow state can be found in RFC 1765.

To enable database overflow follow the steps below

Enter ospf router configuration mode

```
Configure router ospf <enter>
```

Enable database overflow

```
Set database-overflow enable <enter>
```

Set the number of external LSA's that can be stored in a link state database before entering the overflow state. A valid integer is between 0 and 4294967294.

```
Set database-overflow-max-lsas "integer" <enter>
```

Type "end" to save changes

Example

```
configure router ospf
      set database-overflow enable
      set database-overflow-max-lsas 5000
      end
end
```

Stub Area

Configuring your Fortigate to participate in a stub area can also reduce the size of the database as well as the number of SPF calculations. Stub areas reject the flooding of external LSA's into the area.

For Fortigate stub area configuration follow the below steps

Enter ospf router configuration

```
configure router ospf <enter>
```

Enter area configuration

```
configure area <enter>
```

Edit desired area

```
edit area "area_id" <enter>
```

Set area type

```
set type stub <enter>
```

Example

```
configure router ospf
        configure area
          edit 0.0.0.0
                set type stub
                end
end
```

Secure OSPF Configuration

OSPF is not an inherently secure routing protocol, thus there are some security issues that should be discussed. OSPF is not only vulnerable to malicious activity, but administrator mis-configurations as well.

Broadcasting

The default OSPF behavior within a Fortigate is to broadcast LSA updates via multicast. With broadcast mode enabled mis-configurations in routing can be propagated throughout a routing domain. Adjacent devices configured to broadcast can introduce possible malicious route injections.

FortiOS offers multiple network types per OSPF interface including broadcast, non-broadcast, point-to-point, and point-to-multipoint. For our purposes, we will cover the steps necessary to configure non-broadcast mode.

Enter OSPF router configuration mode

```
configure router ospf <enter>
```

Enter interface configuration mode

```
configure ospf-interface <enter>
```

Edit the ospf interface

```
edit "interface name" <enter>
```

Set the network-type to non-broadcast

```
set network-type non-broadcast <enter>
```

Now that non-broadcast is enabled, we must configure our adjacent neighbors.

The following steps are required to configure adjacent neighbors

Enter OSPF router configuration mode

```
configure router ospf <enter>
```

Enter the neighbor configuration sub category

```
configure neighbor <enter>
```

Create a neighbor entry ID in the form of an integer

```
edit "integer" <enter>
```

Specify the IP address of the neighbor router

```
set ip "IP address" <enter>
```

Type “end” to save changes

Example

```
configure router ospf
configure ospf-interface
      edit internal
      set network-type non-broadcast
```

```
        end
    configure neighbor
       edit 1
           set ip 192.168.1.32
       end
end
```

Authentication

By default authentication is not required to receive routing updates into the link state database. This introduces obvious vulnerabilities such as unauthorized route injections and spoofed routing devices.

To enable authentication for an interface follow the below steps

Enter OSPF router configuration mode

```
configure router ospf <enter>
```

Enter the OSPF interface sub category

```
configure ospf-interface <enter>
```

Edit the desired OSPF interface

```
edit "Interface_name" <enter>
```

Set authentication type

```
set authentication md5 <enter>
```

Create an md5 entry and key to be used for authentication

```
set md5-key "integer_id" "md5_key" <enter>
```

Type "end" to save changes.

Example

```
configure router ospf
   configure ospf-interface
      edit internal
          set authentication md5
          set md5-key 1 fortinet
          end
end
```

Access Lists

Although a Fortigate employs stateful inspection firewall functionality, firewall rules are not applied to OSPF routing updates destined for itself. Fortinet does however provide the ability to create access lists to control source and destination routing communication.

To configure OSPF access lists follow the steps below.

Enter the access list configuration sub menu

```
configure router access-list <enter>
```

Create a descriptive access list name

```
edit "access_list_name" <enter>
```

Enter the rule configuration sub menu

```
configure rule <enter>
```

Create access rule number in the form of an integer

```
edit "integer_id" <enter>
```

Specify access list action as permit or deny

```
set action "permit | deny" <enter>
```

Specify network or IP that the action will apply to

```
set prefix "network number" <enter>
```

Type "end" to save changes

Once the access list has been created it is now necessary to apply it to the OSPF area

Enter OSPF router configuration mode

```
configure router ospf <enter>
```

From the ospf# prompt enter the area sub menu

```
configure area <enter>
```

From the area# prompt create the area ID

```
edit "area ID" <enter>
```

Enter the filter list sub menu

```
configure filter-list <enter>
```

Create a new filter list in the form of an integer

```
edit "integer_id" <enter>
```

Specify the direction in which the access list will be applied

```
set direction "in | out" <enter>
```

Specify access list to be applied

```
set list "access_list_number" <enter>
```

Type “end” to save changes

Example

```
configure router access-list
      edit OSPF_ACL
         configure rule
            edit 1
            set action permit
            set prefix 192.168.1.0 255.255.255.0
            end
configure router ospf
      configure area
         edit 0.0.0.0
            configure filter-list
                  edit 1
                  set direction in
                  set list ospf
                  end
end
```

ASBR

It is not recommended to configure your Fortigate platform as an ASBR (Autonomous System Border Router). ASBR’s are used to receive and distribute external routing information. An ASBR will flood external LSA’s throughout non-stub areas. Typically only a single ASBR exists for a single Autonomous System. The implication of this is that routing updates cannot be verified against other ASBR’s. This is in contrast to the behavior of ABR’s where multiple border routers may exist and perform an inherent validation of routing updates.

When configuring a Fortigate as an ASBR is absolutely necessary, enabling database overflow can help with the flooding of excess routes. Additional information on database overflow can be found in RFC 1765.

To configure database overflow parameters follow the below steps

Enter ospf router configuration mode

```
configure router ospf <enter>
```

Enable database overflow

```
set database-overflow enable <enter>
```

Set the number of external LSA’s that can be stored in a link state database before entering the overflow state. A valid integer is between 0 and 4294967294.

```
set database-overflow-max-lsas "integer" <enter>
```

Type “end” to save changes

Example

```
configure router ospf
      set database-overflow enable
      set database-overflow-max-lsas 5000
      end
end
```

Appendix

Extreme Configuration

```
configure ospf add vlan "vlan_192" area 0.0.0.0
configure ospf "vlan_192" authentication encrypted md5 1
"…"
enable ospf export direct cost 10 type ase-type-1 tag 0
enable ospf
```

Cisco Configuration

```
router ospf 1
network 192.168.1.0 255.255.255.0 area 0
router-id 192.168.1.32
```

FortiOS 2.8 Configuration

```
configure router ospf
      set abr-type standard
      configure area
            edit 0.0.0.0
            next
            end
      set default-information-originate always
      configure network
            edit 1
            set prefix 192.168.1.0 255.255.255.0
            set area 0.0.0.0
            next
            end
      configure ospf-interface
            edit "port1"
            set interface "port1"
            set ip 192.168.1.61
            next
            end
      configure redistribute "connected"
            set status enable
            end
      configure redistribute "static"
```

```
      set status enable
      end
configure redistribute "rip"
      set status enable
      end
set router-id 192.168.1.61
end
```

References

- Fortigate 2.8 MR5 Command Line Reference Guide
- RFC 1765
- RFC 2328