**FMC Sinkhole Notes**

The Sinkhole object is another one that is new in version 6.  We will go into detail on how this works in the chapter on DNS and SSL policy.  For now, we will whet your appetite with a brief description of the Sinkhole object and a bit of information on how to create one.

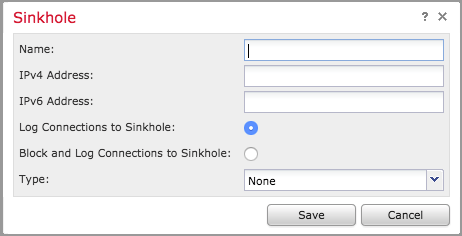
A sinkhole is a DNS server that is designed to return non-routable addresses in response to DNS queries.  More accurately, these IP addresses – routable or not – do not resolve to an actual server.  Since DNS resolution is the first step in virtually any TCP/IP connection, this is designed to prevent a user/host from successfully establishing a connection.  By making it impossible to resolve a name to an IP address, the connection is stopped dead in its tracks.

You might ask, “why not just block the DNS request – why use a sinkhole?”  That’s a good question.  One reason has to do with the placement of the IPS in relation to your internal DNS server.  Often times, the IPS sees a DNS request for an evil domain coming from your DNS server who forwarded it on behalf of an infected client.  (Infected by malware or just infected by a user)  The IPS can easily block this request using a Snort rule however, what you really want to know is – which of my hosts made that DNS query?

Since the host is trying to resolve an “evil” hostname it would be very helpful to know which host this is and maybe send in the incident response team.  By using a sinkhole we can return a bogus IP address to the DNS server who relays that to the (infected) host.  Now when the host tries to actually connect to this sinkhole IP – BAMO – we’ve got him!  The IPS can see this request and generate an alert that somebody is trying to connect to our sinkhole IP.  The only way a host would get this IP address in the first place is if we gave it to him in response to an evil DNS request.

We said this would be a short description so let’s stop here while we’re ahead.  We will explain this further with fancy pictures and diagrams in the DNS and SSL policy chapter.  For now let’s talk about how you would go about setting up a Sinkhole object.

There are no sinkhole objects created by default.  To create one click the Add Sinkhole button.  This will display the dialog shown in Figure 6.23



The options for your sinkhole are:

• **Name** – Friendly name, you can use spaces if desired

• **IPv4 Address** – the IPv4 address.  Pick an address that resolves to something North of your IPS (outside your network) but that no host should ever try to connect to.  One suggestion is to use the IPv4 space reserved for “documentation” according to RFC 5737.  There are three ranges: TEST-NET-1 **192.0.2.0/24**, TEST-NET-2 **198.51.100.0/24**, TEST-NET-3 **203.0.113.0/24**.  While technically public space, some people also use **1.1.1.1** because it’s so easy to pick out when scanning an event view page.  This should be a single IP address entry not a range.

• **IPv6 Address** – IPv6 does not have a specifically reserved range for documentation but given the size of the IPv6 address space you should be able to come up with something unique!

• **Log Connections to Sinkhole** or **Block and Log Connections to Sinkhole** – fairly straightforward, do you want to allow this packet to continue or block it at the IPS?  If you are using an actual server listening on port 53/UDP for your sinkhole IP address you may want to allow the connection so you can log the request there.  Either way Firepower will log it as a Security Intelligence event.

• **Type** – the DNS security intelligence category breaks down into three types:

* o Command and Control (CnC)
* o Malware
* o Phishing

The purpose of this selection is to allow you to have different DNS sinkhole IPs for each type of DNS request.  You may want to prioritize CnC events and remediate these more quickly.  This way you can setup special alerting for any hosts triggering your CnC sinkhole IP.

Once your sinkhole object(s) are added you can use them in your DNS policy to catch more evil on your network!

**Sinkhole Reloaded**

Now that you know how a sinkhole works let’s think of ways we can (ab)use this feature.  Since you can now make the DNS server return whatever IP you want, you control *everything*!  Say, you have a list of sites that you’d rather nobody go to.  Maybe you want everyone to use only your favorite dating site – farmersonly.com.  To implement your evil plan using the DNS sinkhole feature here are the steps to take.

1. Create a text file with all the domains of all those other sites like eharmony.com, match.com, okcupid.com, etc.

2. Upload this file as a custom DNS Security Intelligence object.

3. Create a Sinkhole object and use the actual farmersonly.com site for the IP address (see Figure 6.24).  Make sure you don’t block the connections to this sinkhole.

4. In your DNS policy add a rule with an action of Sinkhole and for the Sinkhole select your Farmersonly-dot-com Sinkhole object.  On the DNS tab add only your custom DNS Security Intelligence object.

5. Deploy policies

What you did is tell the device to sinkhole any request for one of those other dating sites and instead return the farmersonly.com IP address.  The result will be that anyone trying to go to match.com, eharmony.com, etc. will find themselves looking at the farmersonly.com site.  Then get ready for the helpdesk calls!