DuckCorp Infrastructure - Review #711

Allow to connect to services hosted on Orthos while being at Conde

2020-08-25 17:42 - Pierre-Louis Bonicoli

Status:	Resolved	**Start date:**	2020-08-25
Priority:	Normal		
Assignee:	Marc Dequènes		
Category:	System :: Network		
Target version:			
Branch:	allow_input_connections_from_hypervisor		

Description

allow_input_connections_from_hypervisor branch from duckcorp-infra repository.

Allow input connections from the hypervisor

While being at Conde, without this patch, I am not able to reach sup.duckcorp.org. Indeed the following packet is dropped:

On the hypervisor:

```
IP 192.168.100.1.33874 > 192.168.100.2.443: Flags [S]
```

where:

```
192.168.100.1: IP of the hypervisor on the bridge used with libvirt
192.168.100.2: Orthos
```

This patch has been applied already.

History

#1 - 2020-08-25 17:42 - Pierre-Louis Bonicoli

- Status changed from New to In Progress

#2 - 2020-08-25 17:43 - Pierre-Louis Bonicoli

- Description updated

- Status changed from In Progress to Rejected

#3 - 2020-08-25 17:43 - Pierre-Louis Bonicoli

- Status changed from Rejected to In Progress

#4 - 2020-08-28 08:26 - Marc Dequènes

- Assignee changed from Marc Dequènes to Pierre-Louis Bonicoli

The iptables call is fine; indeed RFC1918 are not expected on the WAN interface but Orthos is not directly connected to the Internet.

I just don't understand the check of interfaces count, what is it supposed to prevent?

#5 - 2020-08-28 12:13 - Pierre-Louis Bonicoli

Marc Dequènes wrote:

> I just don't understand the check of interfaces count, what is it supposed to prevent?

The goal is to detect configuration inconsistency, for example if this template were to be reused.

I updated this check:

```
diff --git a/ansible/roles/dc-base/templates/fw/Orthos b/ansible/roles/dc-base/templates/fw/Orthos
index fecc03f..8327e25 100644
--- a/ansible/roles/dc-base/templates/fw/Orthos
+++ b/ansible/roles/dc-base/templates/fw/Orthos
@@ -19,7 +19,7 @@ ban_bad_people_hook()
         fi
     /sbin/iptables -t filter -A INPUT -j bogons
     {# raise an error when network interfaces differ from (lo, default interface) #}
-    {%- if ansible_interfaces|length != 2 %}
+    {%- if ansible_interfaces|length != 2 or ([ansible_default_ipv4.gateway, ansible_default_ipv4.address] |
ipaddr('public')) %}
     {{ undefined|mandatory('unexpected network interfaces: ' ~ ansible_interfaces) -}}
     {% endif -%}
     /sbin/iptables -t filter -I bogons -s {{ ansible_default_ipv4.gateway }} -d {{ ansible_default_ipv4.addre
ss }} -j RETURN
```

#6 - 2020-08-28 12:35 - Pierre-Louis Bonicoli

- Assignee changed from Pierre-Louis Bonicoli to Marc Dequènes

#7 - 2020-09-01 21:25 - Marc Dequènes

- Assignee changed from Marc Dequènes to Pierre-Louis Bonicoli

This check has absolutely nothing to do with the original PR. Moreover these templates are specific parameters and functions to customize *srv_firewalling* already so it is never gonna be reused. Also we setup the interfaces via Ansible so this should never happen. Here this check requires syncing configuration in two places, this one being not obvious at all, thus I believe this is not a good approach.

I would suggest a more descriptive approach of the network config if we want to improve. For example I made changes to handle ppp interfaces in a generic way for Elwing (see host_vars/Elwing/net.yml). In this case we could simply bring bogons support into *srv_firewalling* (no idea why it's duplicated since it's used on all machines) (outside of the hook to still be able to add host-specific config, maybe with a *net.filter_bogons* flag) and add a flag *net.wan_natted* which would trigger this behavior. Anyway, this is for a separate PR.

#8 - 2020-09-01 21:27 - Pierre-Louis Bonicoli

- Status changed from In Progress to Rejected

- Assignee deleted (Pierre-Louis Bonicoli)

#9 - 2020-09-05 03:37 - Pierre-Louis Bonicoli

- Status changed from Rejected to In Progress

- Assignee set to Marc Dequènes

Updated: Following our exchanges on IRC, I removed the first check (about the number of interfaces) and kept only the check about private ranges.

```
diff --git a/ansible/roles/dc-base/templates/fw/Orthos b/ansible/roles/dc-base/templates/fw/Orthos
index 8327e25..33c9853 100644
--- a/ansible/roles/dc-base/templates/fw/Orthos
+++ b/ansible/roles/dc-base/templates/fw/Orthos
@@ -18,9 +18,9 @@ ban_bad_people_hook()
         sh /var/lib/adm/bogons-iptables.sh
         fi
     /sbin/iptables -t filter -A INPUT -j bogons
-    {# raise an error when network interfaces differ from (lo, default interface) #}
-    {%- if ansible_interfaces|length != 2 or ([ansible_default_ipv4.gateway, ansible_default_ipv4.address] |
ipaddr('public')) %}
-    {{ undefined|mandatory('unexpected network interfaces: ' ~ ansible_interfaces) -}}
+    {# raise an error when the IPv4 of the default network interface isn't private #}
+    {%- if [ansible_default_ipv4.gateway, ansible_default_ipv4.address] | ipaddr('public') %}
+    {{ undefined|mandatory('unexpected network setup: ' ~ ansible_default_ipv4.alias) -}}
     {% endif -%}
     /sbin/iptables -t filter -I bogons -s {{ ansible_default_ipv4.gateway }} -d {{ ansible_default_ipv4.addre
ss }} -j RETURN
 }
```

#10 - 2020-09-28 11:55 - Marc Dequènes

Merged. thanks.

#11 - 2020-09-28 11:55 - Marc Dequènes

- Status changed from In Progress to Resolved