Traffic Forwarding: Proxy Chain

This method is suitable for larger organizations with multiple networks that want to direct web traffic through Dome Standard. As the name implies, proxy chaining is used for “chaining” multiple forward proxies to obtain the benefits of
each. Comodo Dome is designed to be placed as the “Upstream Proxy” to other web gateways such as Websense, Bluecoat, iboss and so on.
The following examples use a Bluecoat Proxy SG and Comodo Dome integration scenario, where Bluecoat is downstream and Dome is the upstream proxy.

A. Bluecoat Configuration

1. Basic Chaining

Bluecoat > Dome

In this scenario, Bluecoat Proxy SG is forwarding requests to Dome but performing no authentication. Dome can be
set to do Active Directory authentication.

Use the Blue Coat Management console to forward requests to the Dome as following:

1. In the Blue Coat Management Interface, under the 'Configuration tab', go to Forwading > Forwarding Hosts.
2. Select 'Install from Text Editor' from the drop-down then click 'Install'.
3. Edit the 'Forwarding Hosts' configuration file to point to Dome. e.g:

- Add “fwd_host Dome_Proxy X.X.X.X http=19080” at the end of “Forwarding host configuration” section.
- Add “sequence Dome_Proxy” to the end of “Default fail-over sequence” section4Once editing is complete, click 'Install'.

1. In the 'Configuration' tab, go to 'Policy' and select 'Visual Policy Manager'.
2. Click 'Launch'.
3. In the 'Policy Menu', add a new Forwarding Layer with a chosen policy name.
4. Select the Forwarding Layer tab that is created. Edit source, destination and service columns with
5. necessary information. You can also leave as 'Any' by default.
6. Select the alias name you created in steps 2-5 (e.g: Dome_Proxy) from the list.
7. Click OK.
8. Click Install Policy

2. X-Authenticated-For Chaining

In this scenario, Bluecoat will be configured to pass X-Authenticated-User headers to Dome Proxy and Bluecoat will

be doing user authentication as the downstream proxy.

Editing Bluecoat local policy file:

1. Go to the 'Configuration' tab.
2. Click 'Policy' in the left column and select 'Policy Files'.
3. Edit the text file as following:

<Proxy>
action.Add[header name for authenticated user](yes)
define action dd[header name for authenticated user]
set(request.x_header.X-Authenticated-User, "WinNT://$(user.domain)/$(user.name)")
end action Add[header name for authenticated user]

Or use the Visual Policy Manager

1. Go to the 'Policy Menu' and select 'Add Web Access Layer' and give the policy a name
2. Set Source, Destination, Service and Time column as 'ANY'
3. Right click on 'Set' and click 'New' then 'Control Request Header'
4. Enter X-Authenticated-User in the 'Header Name' field.
5. Select 'Set Value' radio button and enter: WinNT://$(user.domain)/$(user.name)
6. Click 'OK'.
7. Click 'New' and select 'Combined Action Object', enter a name, select the previously created headers and
8. Click 'Add'.
9. Click 'OK'.
10. Click 'Install Policy'.

After connecting your network(s), make sure to add them as a 'Trusted Network' in the 'Locations' interface. If you do
not then Dome will not function correctly and your network will not be able to connect to the internet. Refer to 'Managing Trusted Networks' for more details.
Please contact us at domesupport@comodo.com if you have any issues connecting endpoints / networks to Dome Standard