The XRIO V-BOND Solution

XRIO V-BOND allows service providers to build their core IP Bonding infrastructure based on any Virtualisation platform that supports the use of the Open Virtual Format (OVF) Standard such as VMWare and Citrix Xen Server. Through the use of Virtualisation technologies, it is possible to build highly scalable, highly resilient services offerings that can grow with customer demand.

Possible Deployment Scenarios

The Xrio V-BOND Solution can enable the deployment of an end-user solutions explained below.

IP Bonding

Enables true aggregation for any type of IP circuit within the ISP network. The V-BOND Instance simply installs in the same way you would a hosted server. Simply allocate the UBM appliance an IP address and gateway together with a routed range that will be used to provision at the customer premise.

Bonded IPVPN

Can be used to provision multi-site IPVPN's with multiple circuits at the customer presence. The V-BOND instance will provide routing to all connected sites. If the destination network resides on a separate V-BOND instance or perhaps does not perform part of the Bonded IPVPN, the traffic is simply forwarded to gateway to make a routing decision.

Mixed Private and Public Circuits

An increasing trend is for businesses that are currently maintaining private circuits such as MPLS, to seek increased bandwidth, scalability and reliability through the use of lower-cost DSL connectivity whilst maintaining the service levels provided by their current connectivity. The UBM appliance allows the possibility to mix private and public circuits using potentially different technologies to form a secure, reliable IPVPN.

Provisioning the V-BOND Core Infrastructure

Connecting your Hardware Platform

Connecting the V-BOND service to your core network can be done in several ways depending on your requirements.

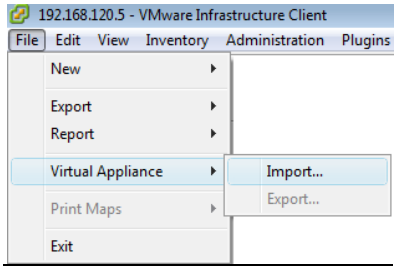
1. A single cable from the hardware platform into your core switching infrastructure (most common).
2. A cable from your hardware platform for each of the V-BOND Instances.
3. Two cables from your hardware platform, one connecting to the access gateways such as ADSL, and one to Internet transit.

UPLOADING THE V-BOND VIRTUAL APPLIANCE

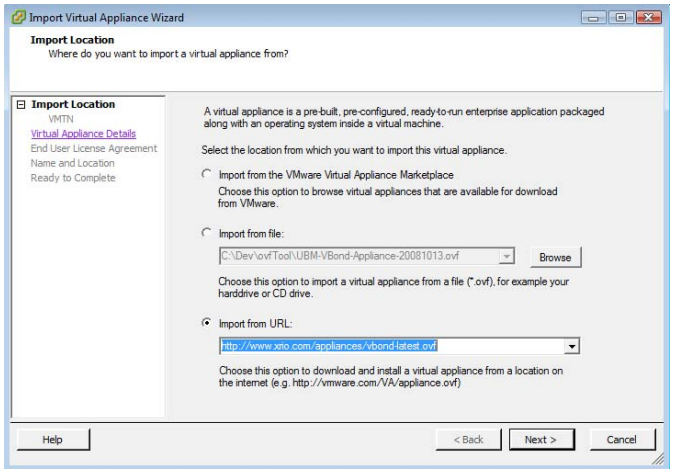
Once you have physically connected the hardware platform to your network you are ready to upload your virtual instance to the virtualisation platform. This is provided using a Open Virtual Format (OVF) Standard image that can be downloaded from the XRIO website.

Using VMWare ESX

1. Open Virtual Infrastructure Client and select the Virtual Server you wish to use for deployment.
2. From the File Menu, choose Virtual Appliance and then Import.

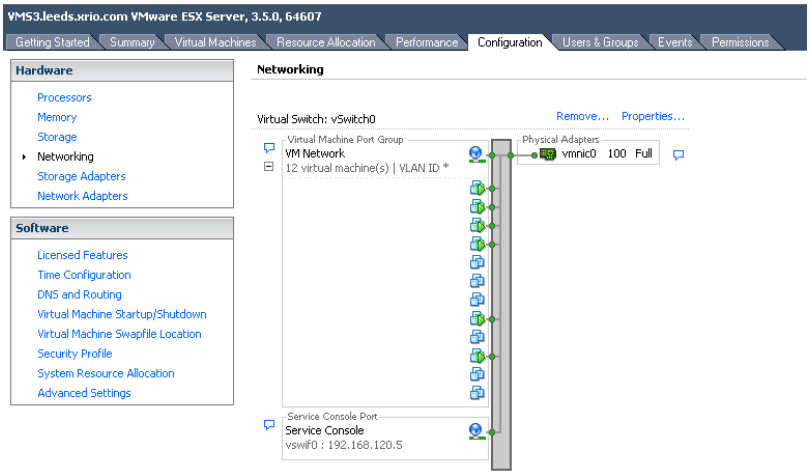


3. Now you need to select the Virtual Appliance file you want to import. You have 2 options here. You can download the latest OVF file from http://www.xrio.com/appliances/vbond-latest.ovf and save it to disk or you can use the Virtual Appliance Wizard to download it directly.

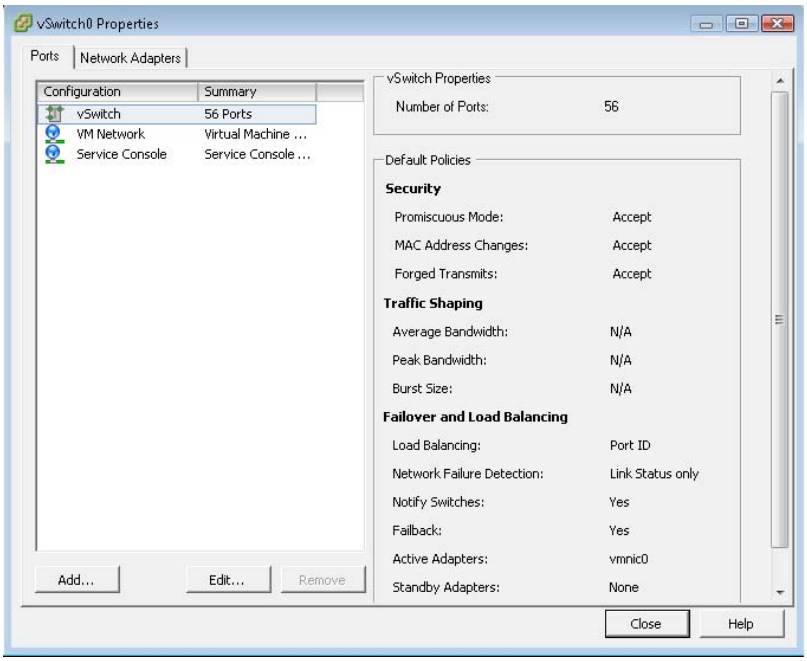


4. Follow the Virtual Appliance Wizard to the end to install the V-BOND appliance to your ESX server.
5. Once V-BOND is installed, we need to set some security options on the ESX Server.

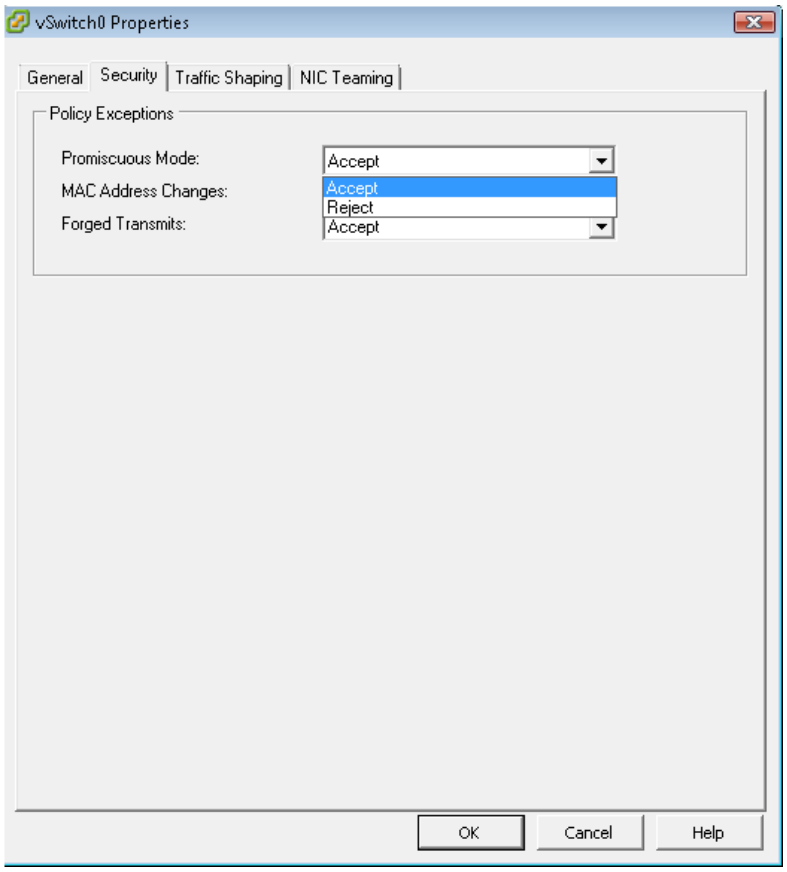
    a. Select the ESX Server on which you have installed the V-BOND appliance, and select the Configuration tab.



b. On the Virtual Switch click Properties.



c. Select the vSwitch and then click Edit.



d. Now choose the Security tab and change the Promiscuous Mode to Accept.
e. To complete accept the changes by clicking OK.

6. Start the Virtual Appliance.
7. We now need to configure your V-BOND appliance.

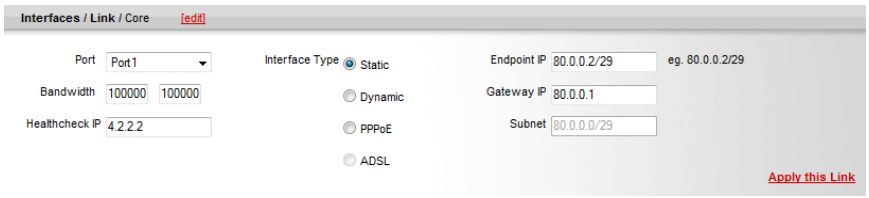
CONFIGURING YOUR V-BOND APPLIANCE

Once your V-BOND appliance is operational we now need to configure the initial IP address and routing information in order to upload the licensing information and initial configuration.

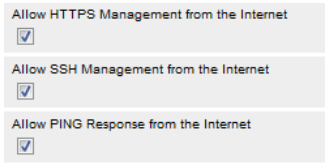
1. From the Video Console inside Virtual Infrastructure Client, login to the V-BOND appliance using the username of admin and password of 123.
2. Once you have logged in set the IP address, default gateway and port number using the following command:

```
set ip address x.x.x.x/y x.x.x.x n
eg. set ip address 80.0.0.2/29 80.0.0.1 1
```

3. You should now be able to contact the V-BOND appliance using its web browser interface at https://x.x.x.x The default username is admin and password is password.
4. One the left hand side of the dashboard is the MAC address of this device, this is needed to license the V-BOND appliance. Copy this to your clipboard and browse to http://portal.xrio.com/request-license.aspx and enter the relevant information.
5. Once you receive your license file, browse to the Settings tab on the Xrio UBM Management Console and choose Licensing. Browse for your license file and click Upload. If the upload was successful you should see your new license information.
6. On the Configure tab, choose Links. From the toolbar, choose Add a Link. Here you need to configure an IP address and gateway that will be used for management and to terminate connections from the customer premise.



7. Finally, we need to enable remote management. Choose Remote Access from the Management group and check the available options.



8. From the top right hand corner of the toolbar, click Commit Changes and then Write Configuration to Flash.
9. Reboot.
10. Your V-BOND appliance should now be contactable after reboot with the licensing and configuration previously uploaded. You are now ready to use your V-BOND appliance in production.

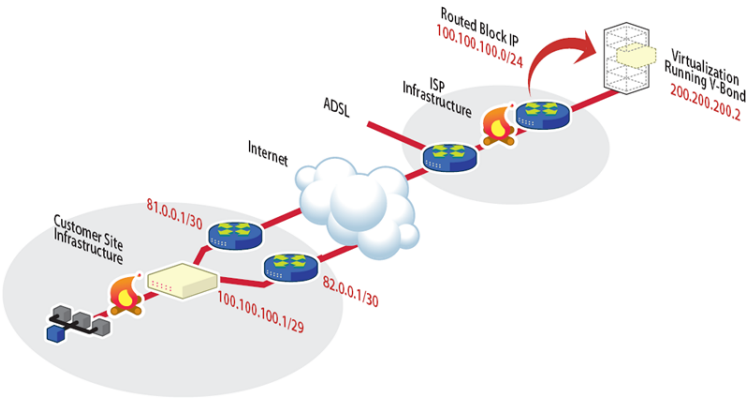
Configuring the Required Routing

If you plan to use this V-BOND appliance for bonding to the Internet or for an IPVPN that spans multiple V-BOND instances, you will need to setup routing information in the core network.

This is done by routing an IP subnet block to the previously configured IP address.

NOTE: The routed IP range and the V-BOND appliances' management address should not form part of the same IP subnet.

The following illustration shows how a typical deployment should look.



Deploying your first Customer

The basic elements of this procedure are as follows.

1. Create Policy on the central UBM appliance to route traffic to the Internet and to the remote site.
2. Create Virtual Tunnel's from each of the remote site links to the central V-BOND appliance.
3. Create Policy on the remote UBM appliance to route all traffic to the central V-BOND appliance.

ON THE CENTRAL UBM APPLIANCE

Create a Link using the IP address and gateway you assigned above.

1. Create Virtual Tunnels for each of the remote site links.
2. Create a Team including the above Virtual Tunnels and select the Simple Bonding algorithm.
3. Create an Address Alias for the Remote Subnet that you are allocating to this customer site. This is usually a small subnet of the previously allocated eg. /29 or /30.
4. Create an Outbound policy to tell the UBM how to route traffic to the Internet as follows:

Source	Any
Destination	Any
Service	Any
Team	Link 1
Translate	Network Address Translation should be Disabled.

5. Create an Outbound policy to tell the UBM how to route traffic to the Internet as follows:

Source	**Any**
Destination	The Address Alias you created in step 4.
Service	Any
Team	The Team you created in Step 3.
Translate	Network Address Translation should be Disabled.

6. Commit and Write the changes to Flash.

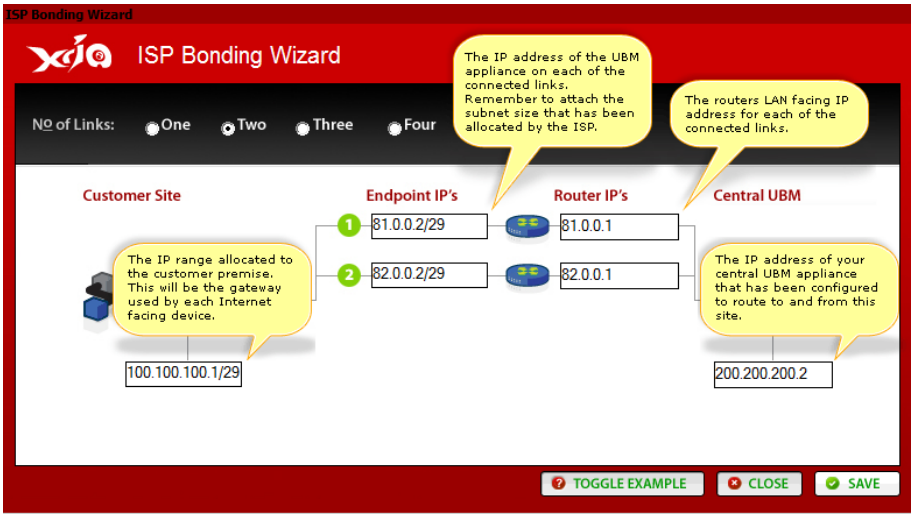
ON THE REMOTE UBM APPLIANCE

You have two options when configuring the remote UBM appliance, by the quick start wizard or manual configuration.

First follow the UBM Appliance Quick Installation Guide, to get you connected to the UBM appliance Management Console.

Quick Start Wizard

It is recommended that you use the ISP bonding Wizard that is shown on the Dashboard of the UBM appliance Management Console. This will create the required configuration and is the quickest way to deploy.



Manual Setup

If you want to create a custom setup or prefer to enter the configuration manually, you can use the Configure tab to enter all your required configuration information.

1. Configure a Link for each of the connected circuits.
2. Create Virtual Tunnels for each of the links terminating on the central UBM appliance reversing the Local/Remote Endpoint and Virtual IP's you assigned.
3. Create a LAN Interface for the subnet you have allocated to this customer. Usually you will assign the first available IP to the UBM appliance itself and the remaining to the connected devices such as a firewall.
4. Create a Team including the above Virtual Tunnels and select the Simple Bonding algorithm.
5. Create an Outbound policy to tell the UBM how to route traffic to the Internet as follows:

Source	Allocated LAN Subnet
Destination	Any
Service	Any
Team	The Team you created in Step 4.
Translate	Network Address Translation should be Disabled.

6. Commit and Write the changes to Flash.
7. Finally, verify the Virtual Tunnels are active in the Live Link Monitor and that you can route to the Internet from a device attached to the UBM appliances' LAN Interface.