APPENDIX A

Recommended Practices and Caveats

The following sections define best practices and caveats.

Recommended Practices

The following recommended practices are results captured by the validation team during the testing cycles and are believed to enhance the experience of Cisco Intercloud Fabric solution at the time of completion of this document. It is important for customers to be up-to-date on the latest features, capabilities, and new recommendations as the product evolves.

Application Deployment Validation for Hybrid Environments

Prior deployment application verification can help verify whether an application is a good fit for a hybrid cloud placement. Things to consider before deployment include:

- Latency minimums between displaced application tiers
- Processor and memory requirements
- Disk requirements that can include specifics for shared or quorum disks
- Bandwidth requirements of the application

Network Planning for Cisco Intercloud Fabric

Network planning to use Cisco ICF requires certain ports to be open as detailed in the Getting Started Guide, but also certain steps should be considered for laying out network segments that are used.

- The VMM (vCenter) are registered with ICFD but PNSC also needs to communicate with the underlying hypervisor hosts managed by that VMM to be able to push images to the hosts.
- ICF components (ICFD, PNSC, cVSM, ICX, ICS) do not need to be on the same network but need to have at least L3 reachability between each other, and IcfCloud need to extend the network hosting the ICS management interface.
- The ICS and the ICF Firewall need to have a VLAN allocated for communication between them. It is only for communication between them, so it does not need to have an Enterprise or ICF Cloud side gateway interface supporting it, nor does it need to have any presence within the Enterprise switching network. Include it in the trunk shared between the ICX and the ICS, and define a port profile for it on the cVSM.

- Deploy an ICF Router if ICF extended networks are communicating with each other. If inter-VLAN routing is not enabled through the deployment of an ICF Router, traffic between cVMs sitting on different ICF extended networks trombones back to the Enterprise to communicate amongst each other.
- IP planning should require four IPs per IcfCloud if using redundant ICX and ICS pairs, as well as at least one additional IP per ICF service component used.
- Catalog instantiated cVMs needs IP blocks allocated to them if they are not utilizing DHCP.
- During the configuration of the ICF Firewall, open AD and DNS required ports to all dependent cVMs that communicate back to the Enterprise for these resources.

Naming Convention

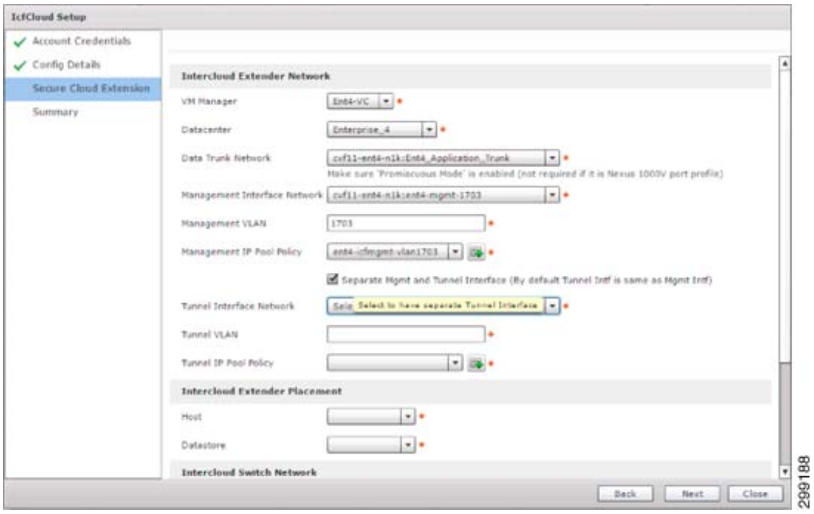
Specifying a descriptive VM Name Template macro within the System Policy helps keep instantiated cVMs more identifiable. System Policies are needed for each vDC and, by default, are set as vm-${SR_ID}, where SR_ID would be the Service Request ID of the VM instantiation request from catalog.

High Level Security Recommendations

Security recommendations for ICF include specifying a Tunnel Interface if connectivity to the provider is broken off from normal management traffic, and setting IP Group configuration within ICFD to push ingress traffic refinement at the provider.

ICF Tunnel Interface is an optional interface that is configured on the ICX for traffic communicating externally to reach the ICS. This interface is enabled within the IcfCloud creation process under Intercloud > IcfCloud > Setup wizard within the Secure Cloud Extension Screen (Figure A-1).

Figure A-1 Addition of Tunnel Interface During IcfCloud Setup

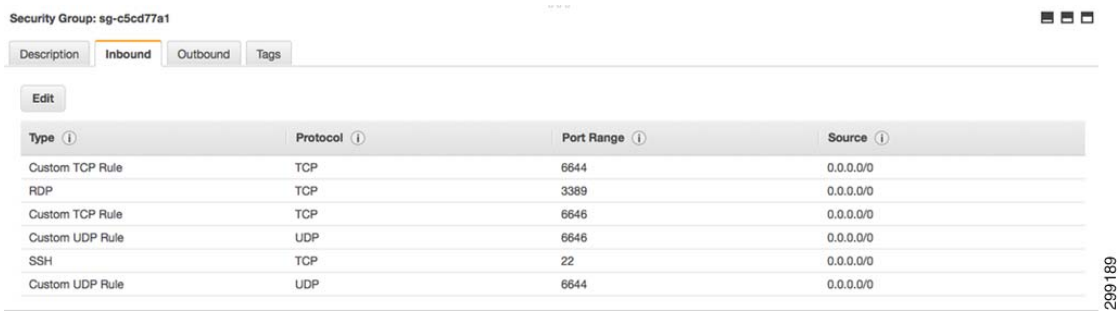


To configure this interface, the Advanced checkbox must be selected as shown in Figure A-1, and then the Separate Mgmt and Tunnel Interface checkbox is selected to pop-up the options for this interface.

This allows the option for a more secure path to be established for this interface if there is an option to set it apart from the management traffic of the other ICF components.

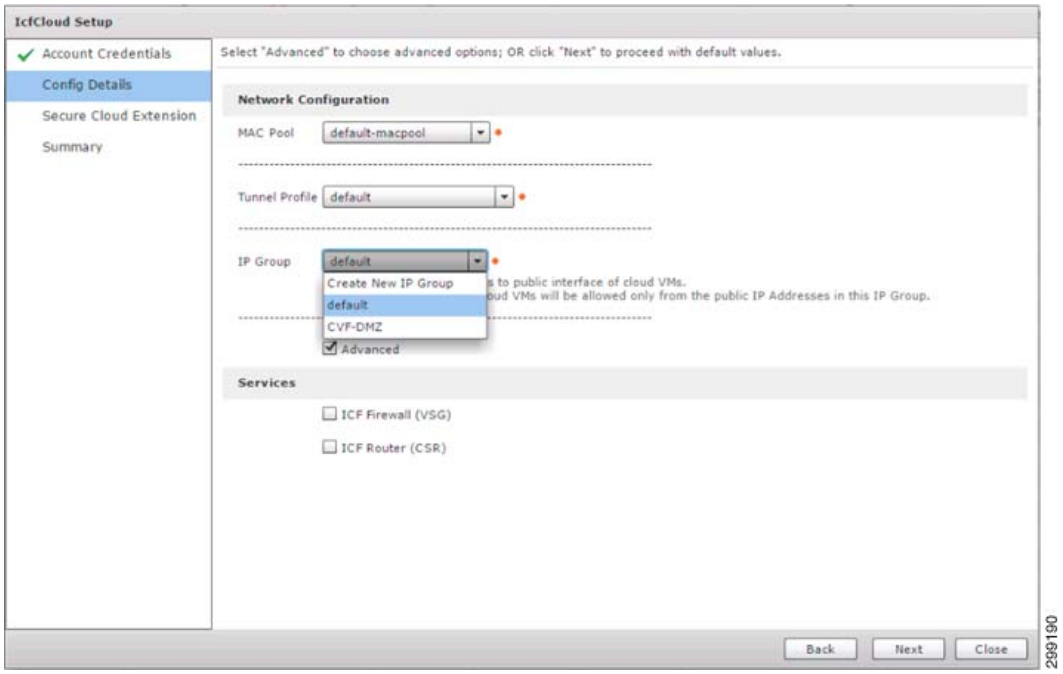
IP Groups specify an IP block, or specific hosts that are designated to be accessible to ICF resources in the Provider environment over required ports. Without an IP Group, the default sets something similar to this for the resources provisioned as shown in Figure A-2.

Figure A-2 AWS Network Security Group without an IP Group Applied



This allows through the needed port connectivity, but it is from any source. An IP Group is set up during the IcfCloud creation to reduce the footprint of exposure to resources in the provider Cloud. This is enabled by selecting the Advanced checkbox of the Config Details in the Intercloud > IcfCloud > Setup wizard shown in Figure A-3.

Figure A-3 IP Group Specification During IcfCloud Setup



IP Groups created is a single host or subnet entry, or a comma separated list of resources or ranges that should be allowed to communicate with ICF resources.

Caveats

The following caveats should be noted.

- **ICF Firewall**—The initial release of ICF Firewall was unstable during the tests. Starting with version 2.2.1, which is available by the time of completion of this document, ICF firewall utilizes a significantly different underlying code, resolving the issues that were identified with version 2.1.2. The new version of the firewall was used to successfully accomplish the tests. Bug ID: CSCus81679.
- **cVM Offloading—**When offloading a VM, the administrator or account user has the option to remove the source VM. If the source VM is not removed, the original VM is powered off after the offloading is completed. If at some point a offloaded VM is attempted to be moved back to its original Data Center, change the VM's name, otherwise a duplicated VM exists in the original Data Center.

Note VMs offloaded back to the Enterprise can only be offloaded to a selected host, and not a specific resource pool.