Edge Gateway Reference Guide

Revision 1.0

Table of Contents

Purpose

The purpose of this document is to catalog a group of processes having to do with Edge Gateway management in vCloud. An Edge Gateway functions as both a firewall and a router. The external network access for a vDC is connected to the Edge, and any external or internal networking is done by routing networks through the Edge. This document details how to set up a functioning network scheme within vCloud.

What is an Edge Gateway?

An Edge Gateway is a virtual router and firewall device designed to run in a vCenter Virtual Machine management environment. They are deployed by the ESXi host managed by vCenter, and are accessible via the vCloud interface. Virtual network constructs such as Internal and External Org VDC Networks allow the Edge Gateway to control traffic through a vDC. Edge Gateways route traffic via NAT rules, which translate network addresses from internal to external, and Firewall rules, which restrict or allow the flow of traffic.

Common Edge Gateway Procedures

Common procedures using Edge Gateways include retrieving external IPs, setting up NAT and Firewall rules, and configuring IPSEC VPNs.

Find Edge Gateway IPs

1. Log In to vCloud

See the IaaS Reference Guide for more information on logging in to vCloud. The IaaS Reference Guide can be obtained by contacting GreenCloud Support.

2. Navigate to Edge Gateways

Select the Administration tab, and double-click on the relevant vDC. Then select the Edge Gateways tab.

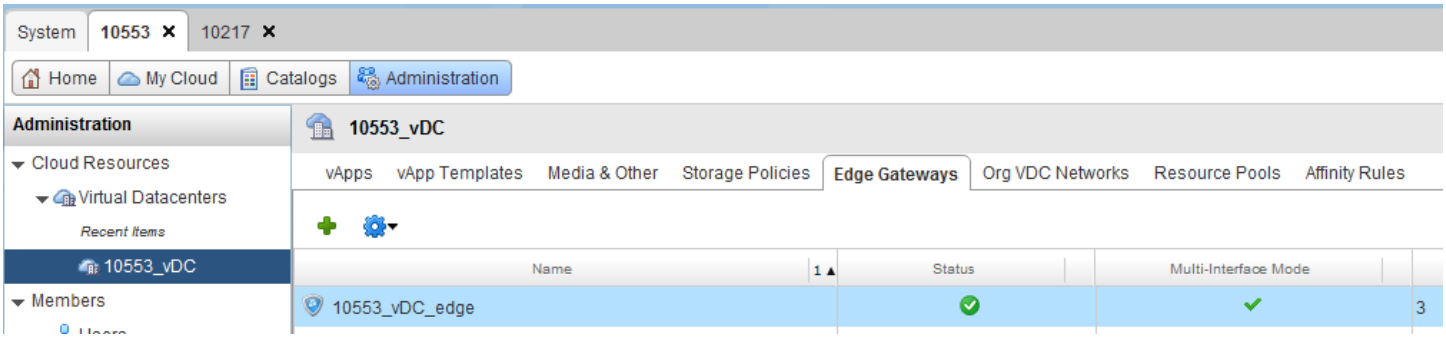


Figure 1 - Edge Gateways

3. Determine External IP Address of Edge Gateway

Right-click on the Edge Gateway and select "Properties". Select the "Configure IP Settings" tab. The "IP Address" tab will list the external IP for that Edge.

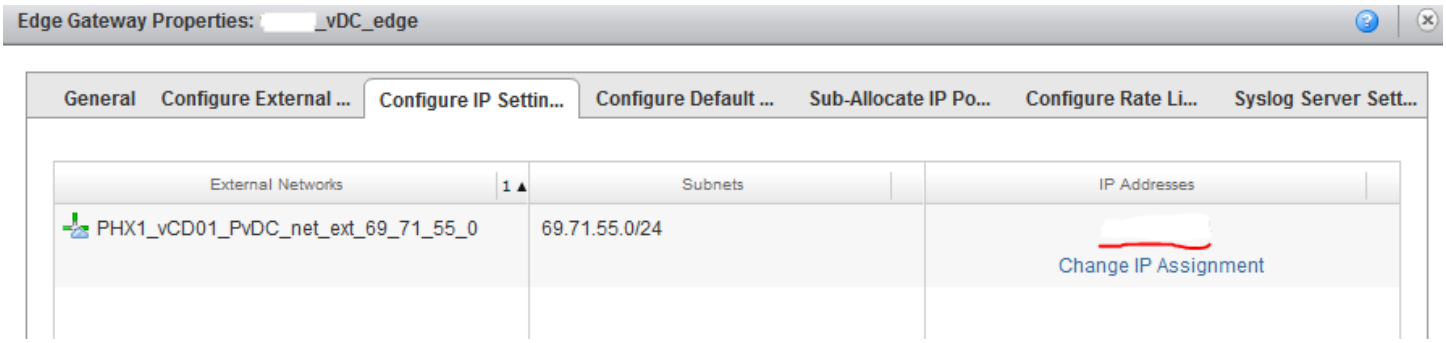


Figure 2 - Edge Gateway External IP

4. Determine All External IP Addresses of vDC

Right-click on the Edge Gateway and select "Properties". Select the "Sub-Allocate IP Pools" tab, then click the External Network, as well as the IP Pool which appears to the right. The box below will list all external IPs which are available for use on that Edge Gateway.

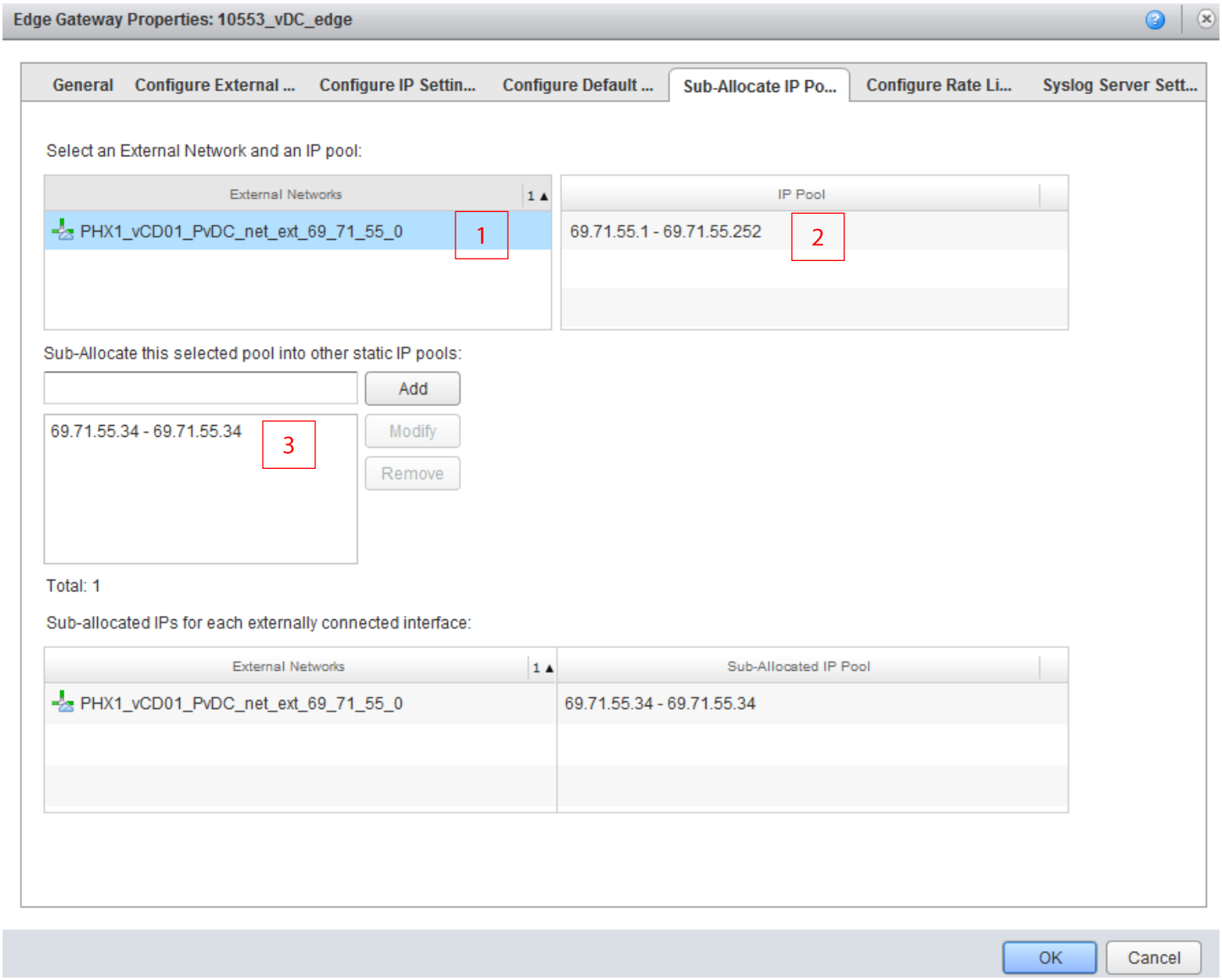


Figure 3 - Edge Gateway Available IPs

Edge Gateway IP Management

If the number of IPs on an Edge Gateway is insufficient, more can be added to a vDC by contacting GreenCloud Support. Most vDCs can support multiple servers on one external IP address by the use of NAT rules and port forwarding. See NAT Rule Management for NAT rule management on Edge Gateways.

NAT Rule Management

Creating NAT Rules

To create a NAT rule, navigate to the Edge Gateway, right-click and select "Edge Gateway Services". Then select the NAT tab.

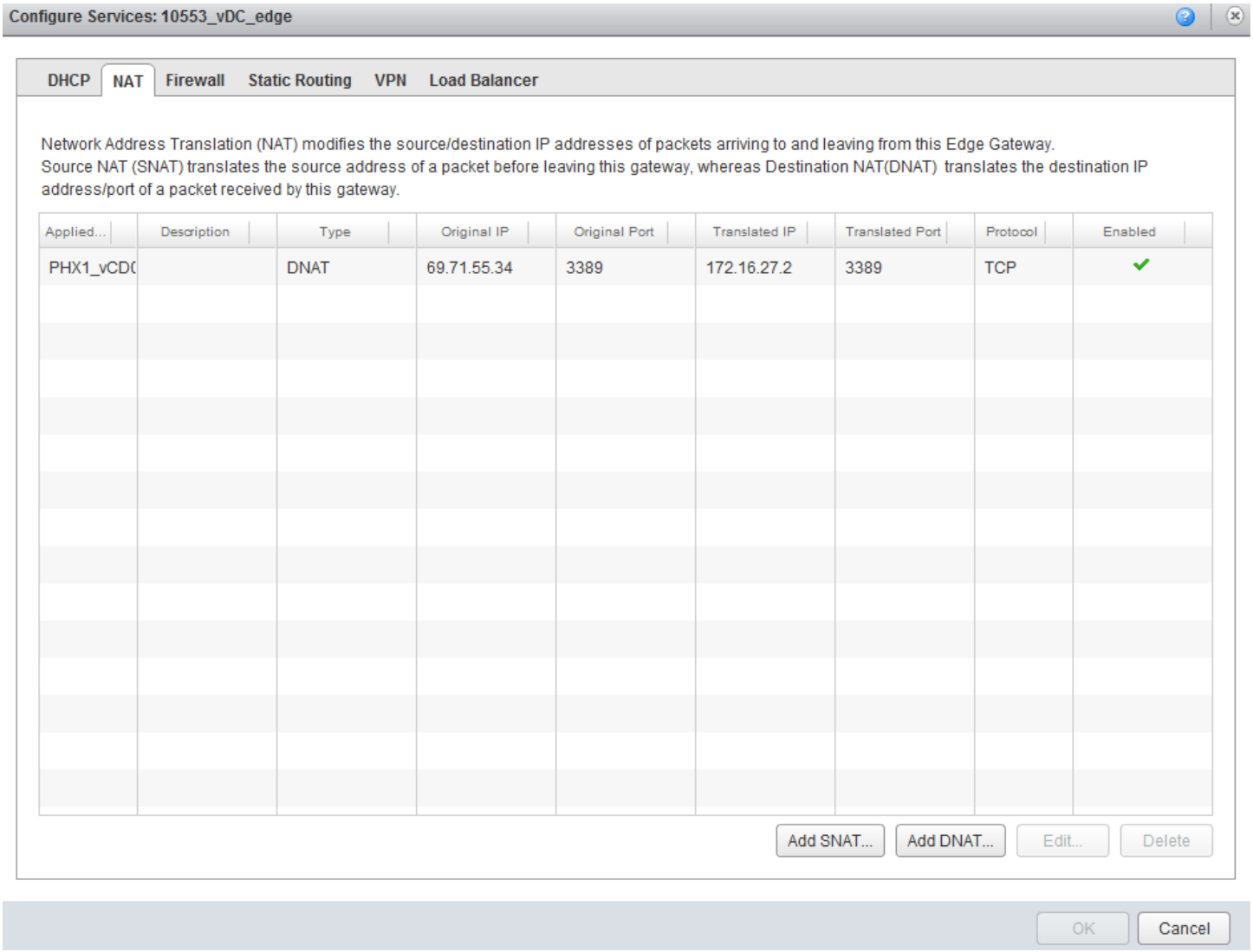


Figure 4 - NAT Rules Tab

The "Add SNAT" button will start the Source Nat dialog, and the "Add DNAT" button will start the Destination Nat dialog. SNAT rules translate the source IP of outbound packets, and DNAT rules translate the destination of inbound packets. At least one of each rule is required in order for traffic to flow across the Edge Gateway into the vDC. Some common examples of necessary NAT rules can be found below. **Note that for any external communication, NAT rules should be applied to the External network (the one containing "EXT" in the name).**

SNAT Rule Example: Many-To-One Outbound

This rule translates the source IPs for all VMs in the vDC to the external IP of the Edge Gateway.

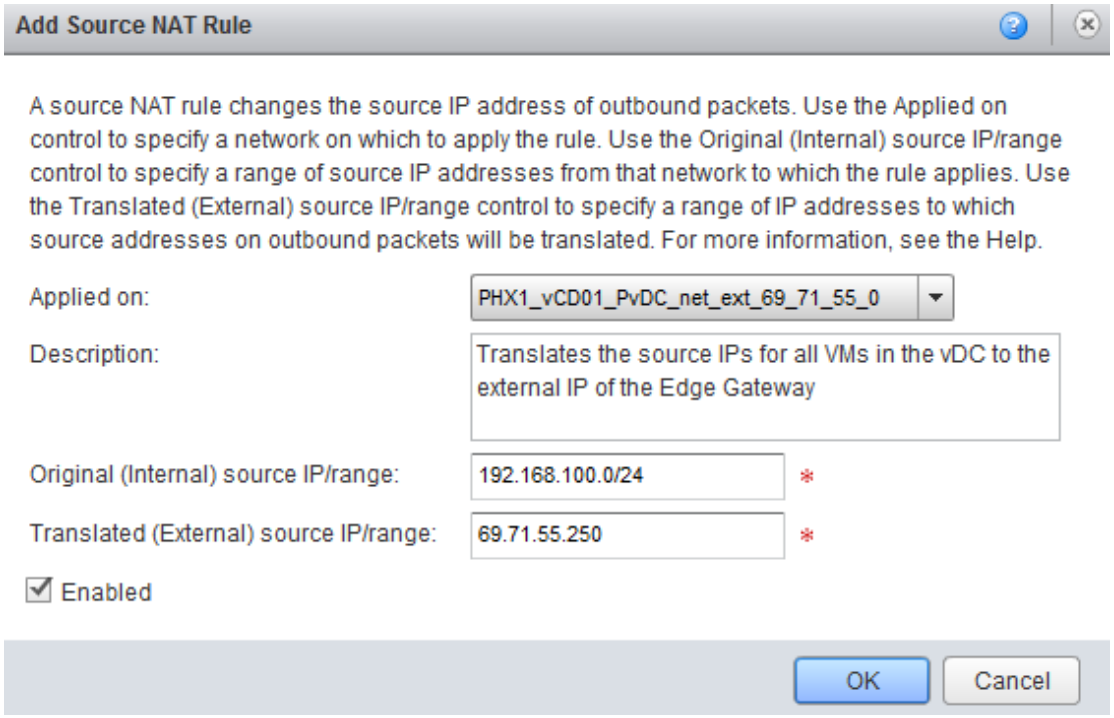


Figure 5 - SNAT Rule Example

Any packet from the subnet 192.168.100.0/24, which is the internal Org VDC network for this vDC, is translated to come from the external IP. **Note that this type of rule is required for a VM to reach the internet.**

DNAT Rule Example: One-To-One Inbound

This rule translates all of the inbound packets for an external IP to go to a specific internal IP.

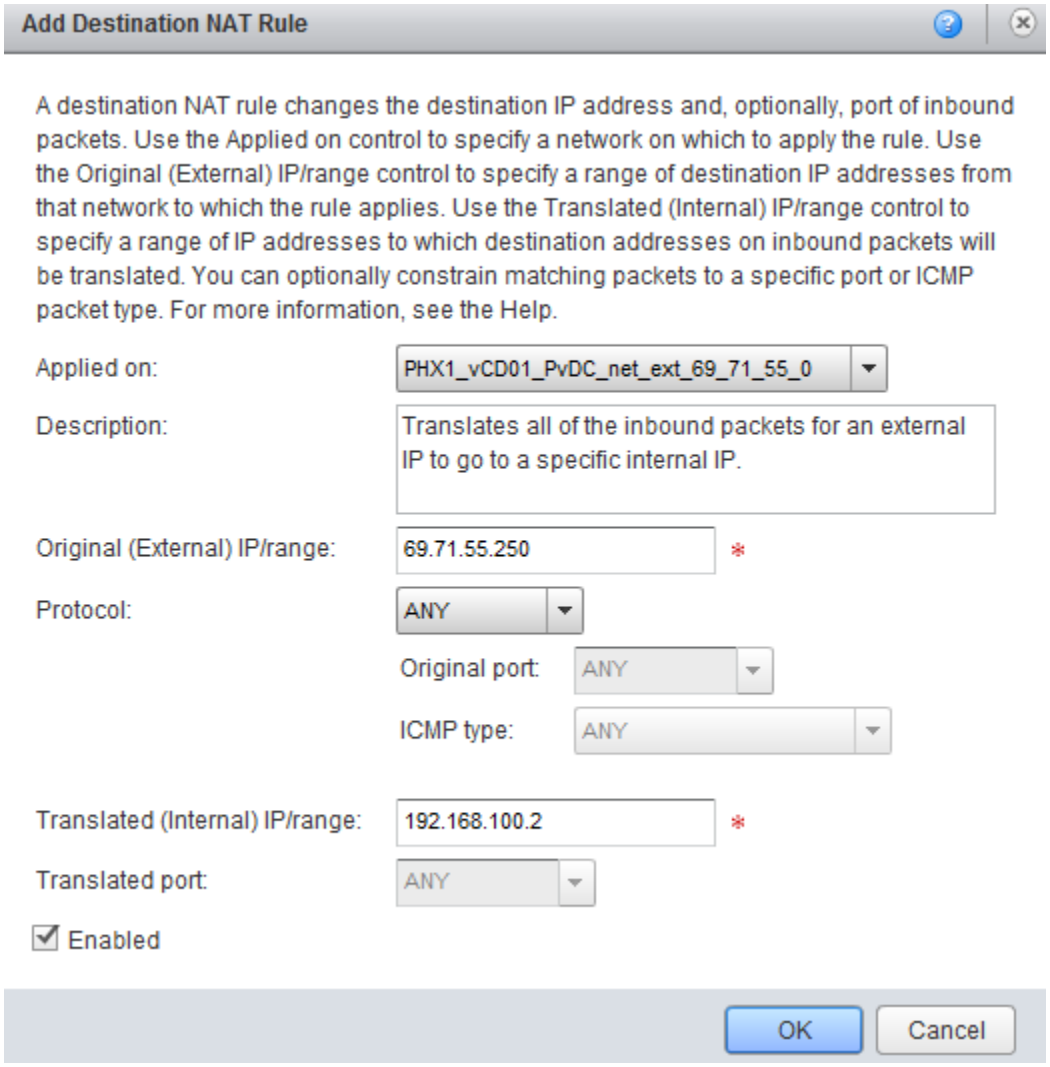


Figure 6 - DNAT Rule Example

This method consumes an entire external IP, and should only be used if a front-facing web server or other application server is hosted in that vDC.

DNAT Rule Example: One-To-One Inbound (Port NAT)

This rule translates the destination IPs for a specific port on the external IP of the Edge Gateway to a specific internal IP of a VM in the vDC.

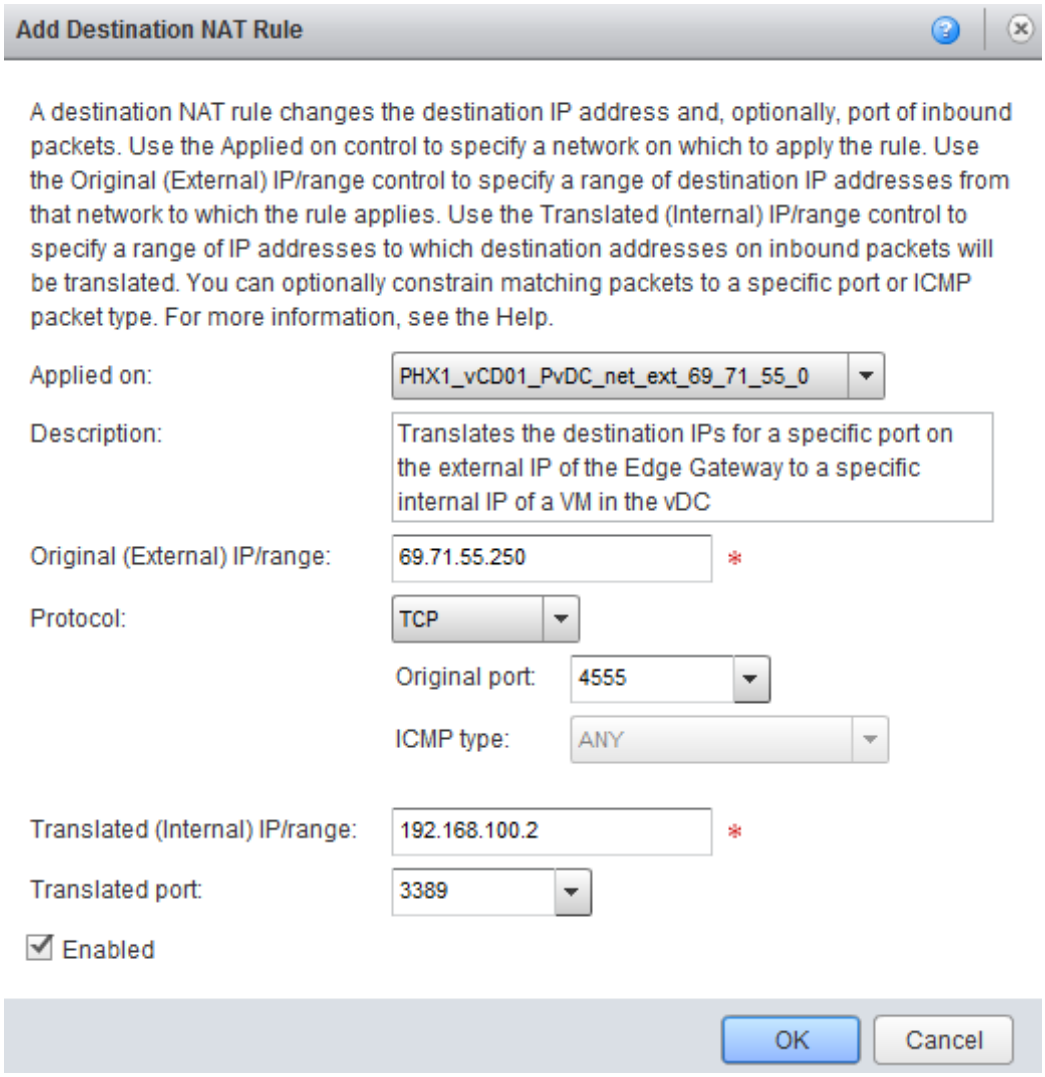


Figure 7 – DNAT Port Rule Example

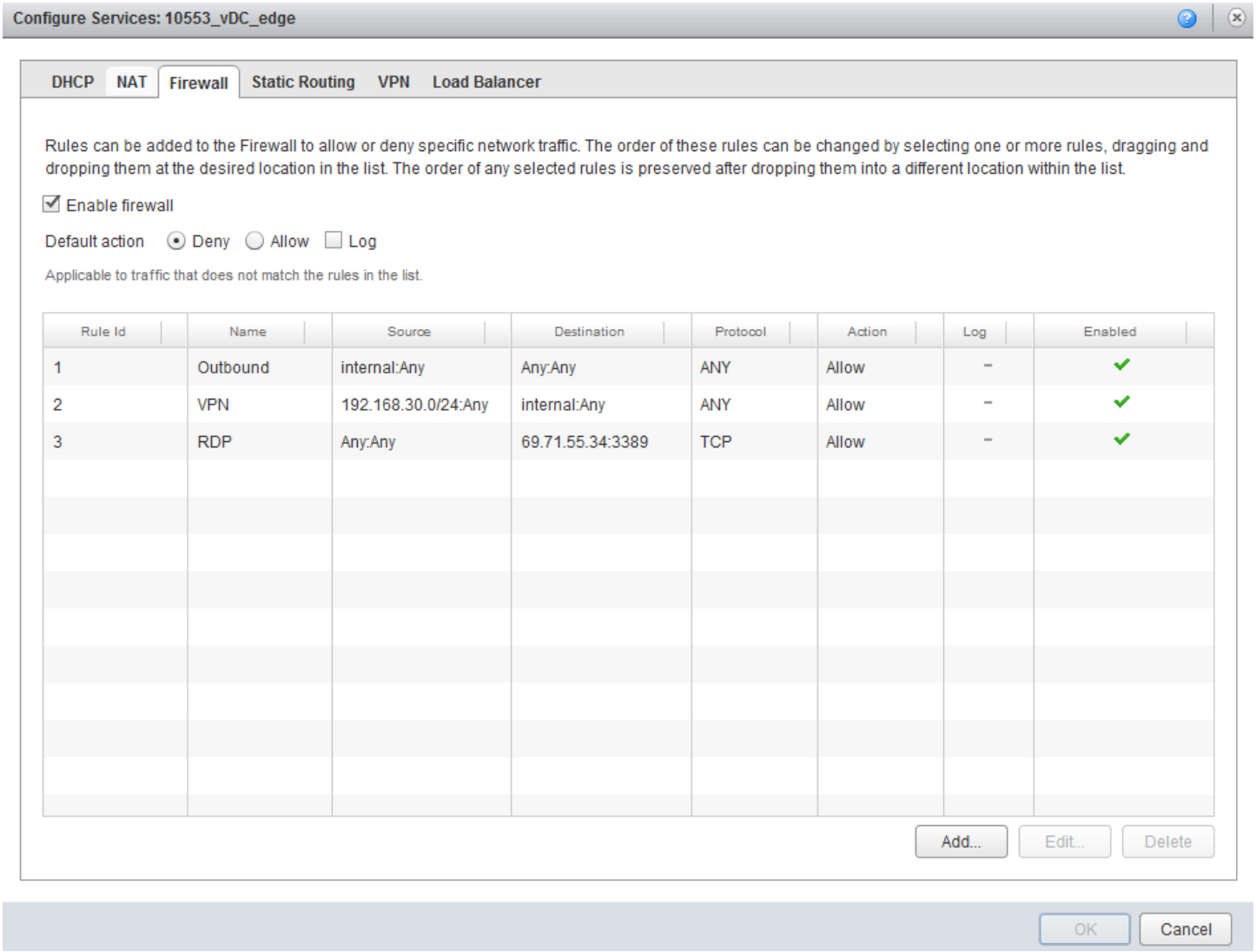
This rule specifically directs the outside port to port 3389 on the internal IP, which allows RDP access.

No matter how traffic is routed the NAT rules must be created, along with corresponding Firewall rules. See Firewall Rule Management for more information on configuring Firewall rules. **Note that this type of rule is necessary to allow traffic to reach a VM.**

Firewall Rule Management

Creating Firewall Rules

To create a Firewall rule, navigate to the Edge Gateway, right-click and select "Edge Gateway Services". Then select the Firewall tab.



The Firewall is enabled by default, and denies all traffic by default. To allow traffic, both outbound and inbound rules are necessary. See below for examples of both inbound and outbound rules.

Firewall Rule Example: Allow All Outbound

This Firewall rule allows all outbound traffic from an internal subnet.

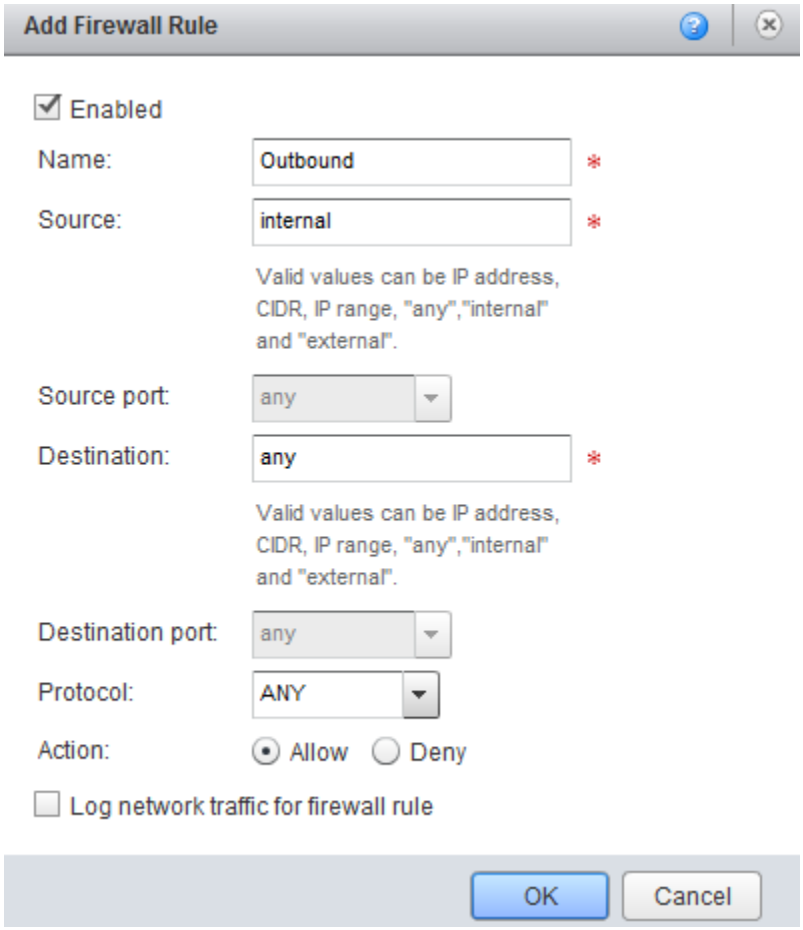


Figure 8 - Firewall Rule Outbound Example

The "internal" keyword refers to any private IP attached to the Edge Gateway. The "any" keyword covers any value for the relevant fields. The action is set to "Allow", which overrides the default "Deny" action.

Firewall Rule Example: Allow Specific Inbound

This firewall rule allows traffic from any source to access the external IP at a specific port.

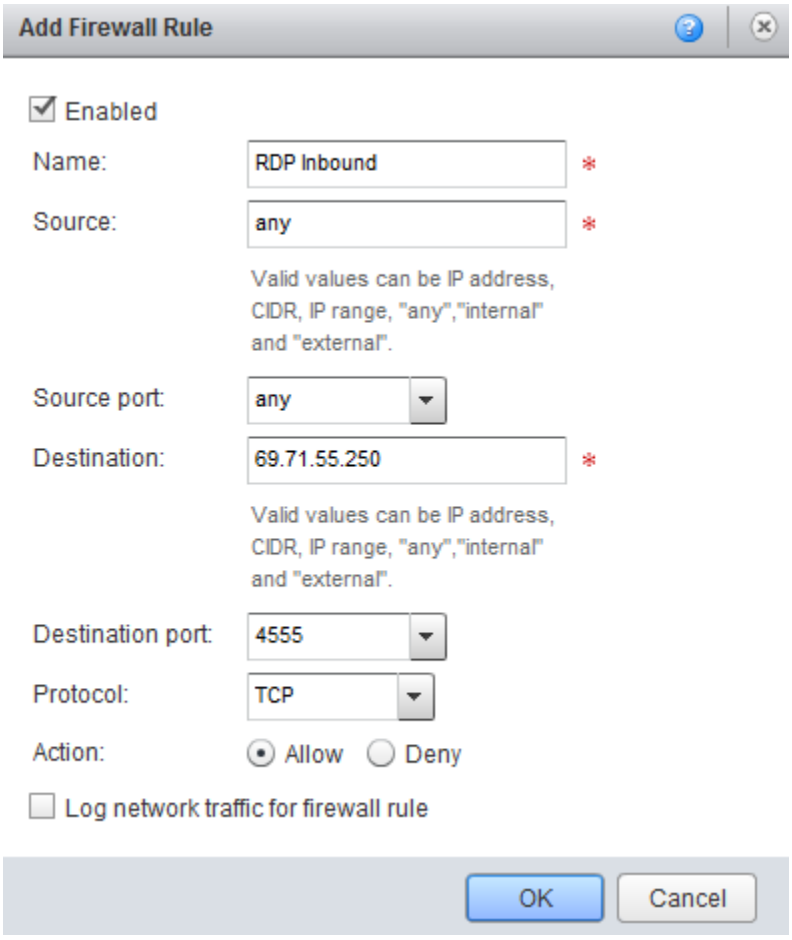


Figure 9 - Firewall Rule Inbound Example

The port should match a port defined by a Port DNAT rule. See DNAT Rule Example: Port NAT for how to set up a corresponding NAT rule.

NAT rules and Firewall rules work together to route traffic across the Edge Gateway. Both are necessary for normal traffic. GreenCloud support is always available for assistance troubleshooting NAT rule interactions.

Firewall Rule Example: Allow ICMP

This Firewall Rule explicitly allows ICMP traffic across to an internal server, which will enable ping traffic. Please note that ICMP ping response is also disabled by default on GreenCloud VMs, so it may be necessary to verify that ICMP is also on for the target server in order to successfully ping.

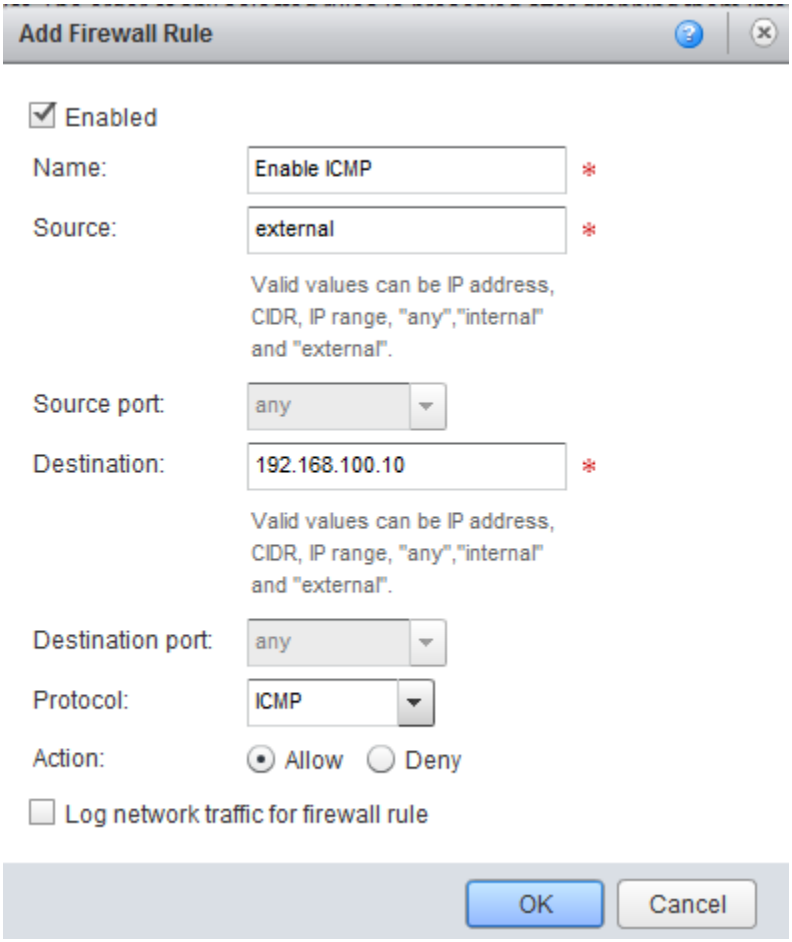


Figure 10 - Firewall Rule Example: Allow ICMP

This rule will allow ping traffic to flow to the target internal IP from an external source.

IPSEC Site-To-Site VPN Configuration

Please note that an IPSEC VPN capable device must be installed at the remote site in order to configure this type of VPN. If there is no VPN capable device at the remote site, no site-to-site VPN can be deployed on the Edge Gateway.

1. Begin VPN Creation

The Edge Gateway can also negotiate and manage VPN connections. To create a VPN, navigate to the Edge Gateway, right-click and select "Edge Gateway Services". Then select the VPN tab.

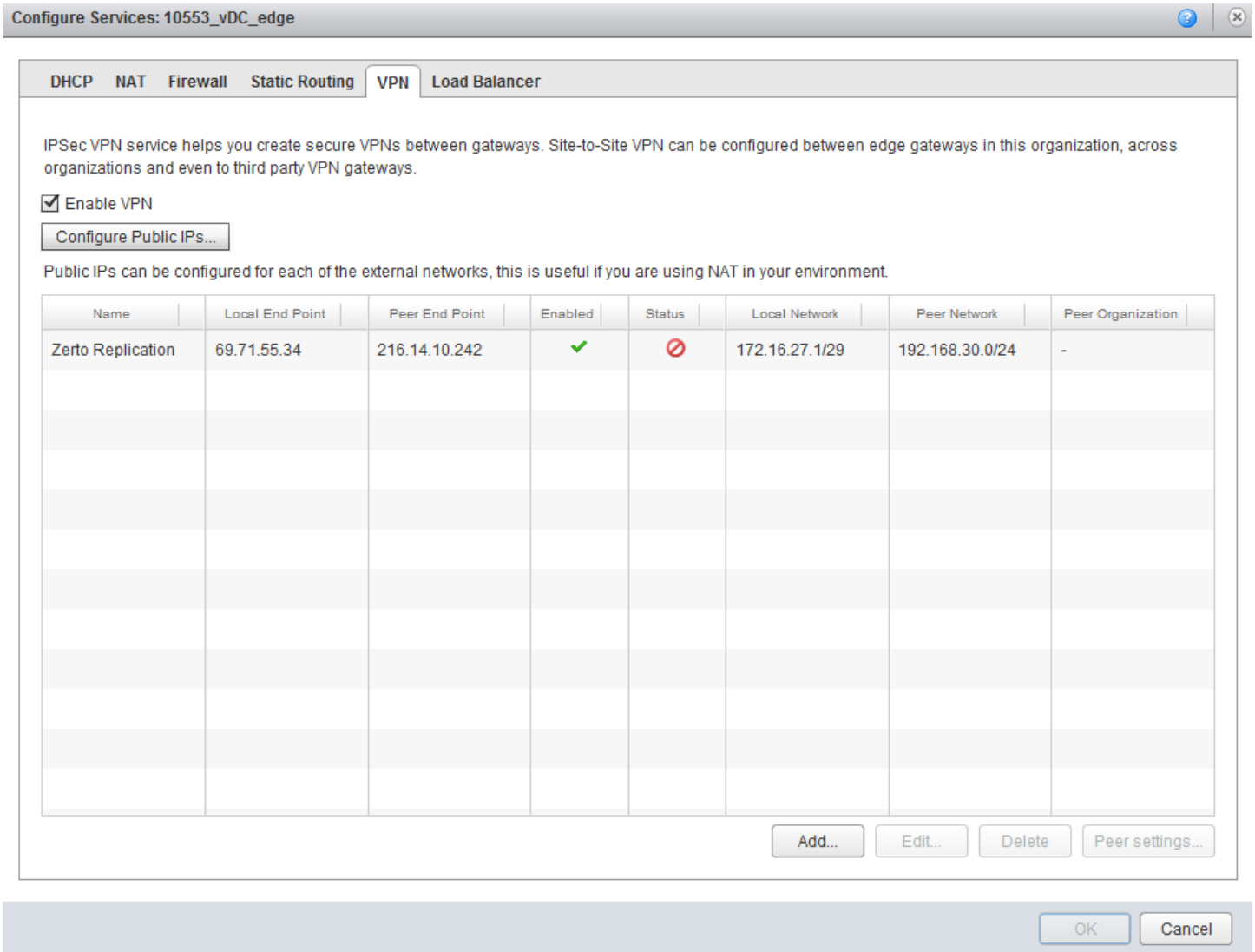


Figure 11 - Edge Gateway VPN List

The VPN service ("Enable VPN" checkbox at the top) is disabled by default to consume resources. Check this box before adding a VPN. Then select "Add" to begin the configuration process.

2. VPN Configuration

Name the VPN and specify that the VPN will go to a remote network, as shown below.

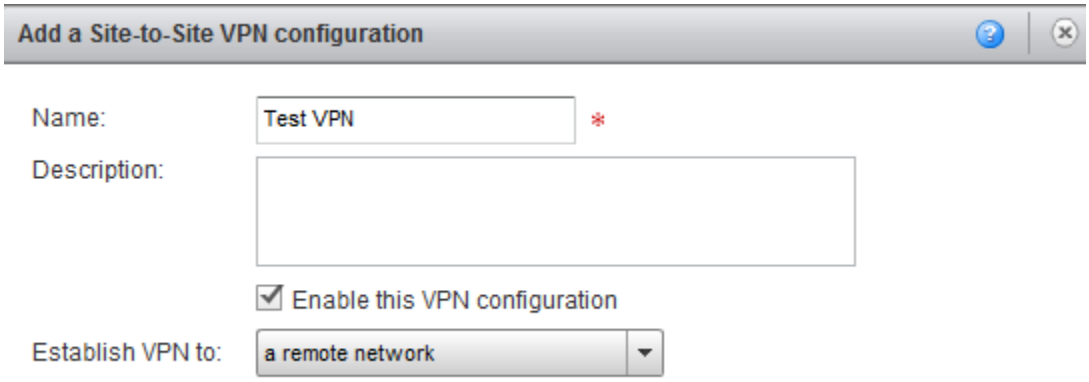


Figure 12 - VPN Configuration 1

Select a Local network to map to the VPN. This should generally be the internal network for the vDC, the same network on which the VMs are addressed. Add the Peer Networks, which will be connected to that subnet. This should be the internal network at the remote site on which the client devices are addressed. Please note that the subnets are not allowed to duplicate any existing subnet on either site.

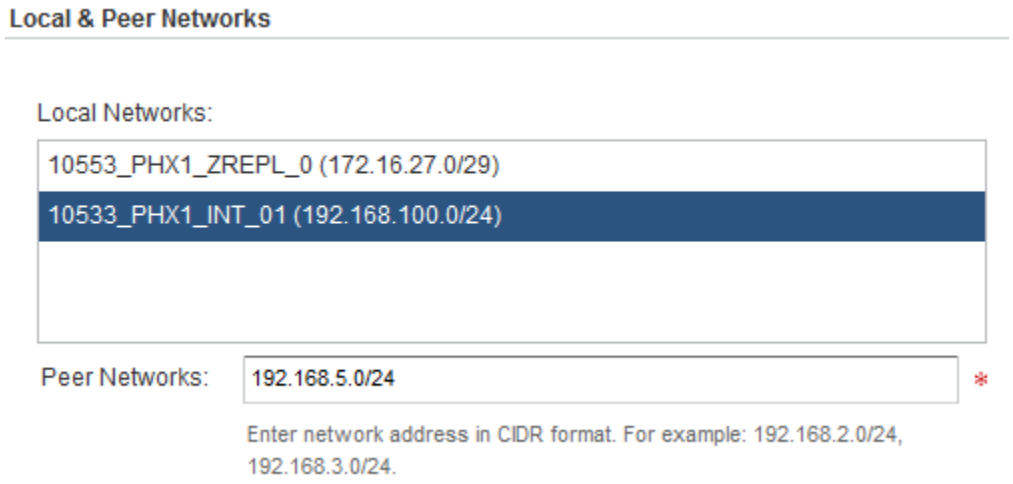


Figure 13 - VPN Configuration 2

Select the Local Endpoint, which should be the external network connected to the Edge Gateway, and input the Local ID, which should be the specific external IP for that Edge Gateway. Set the Peer ID and Peer IP to both be the external IP for the remote site. The Pre-Shared Key can also be entered at this stage.

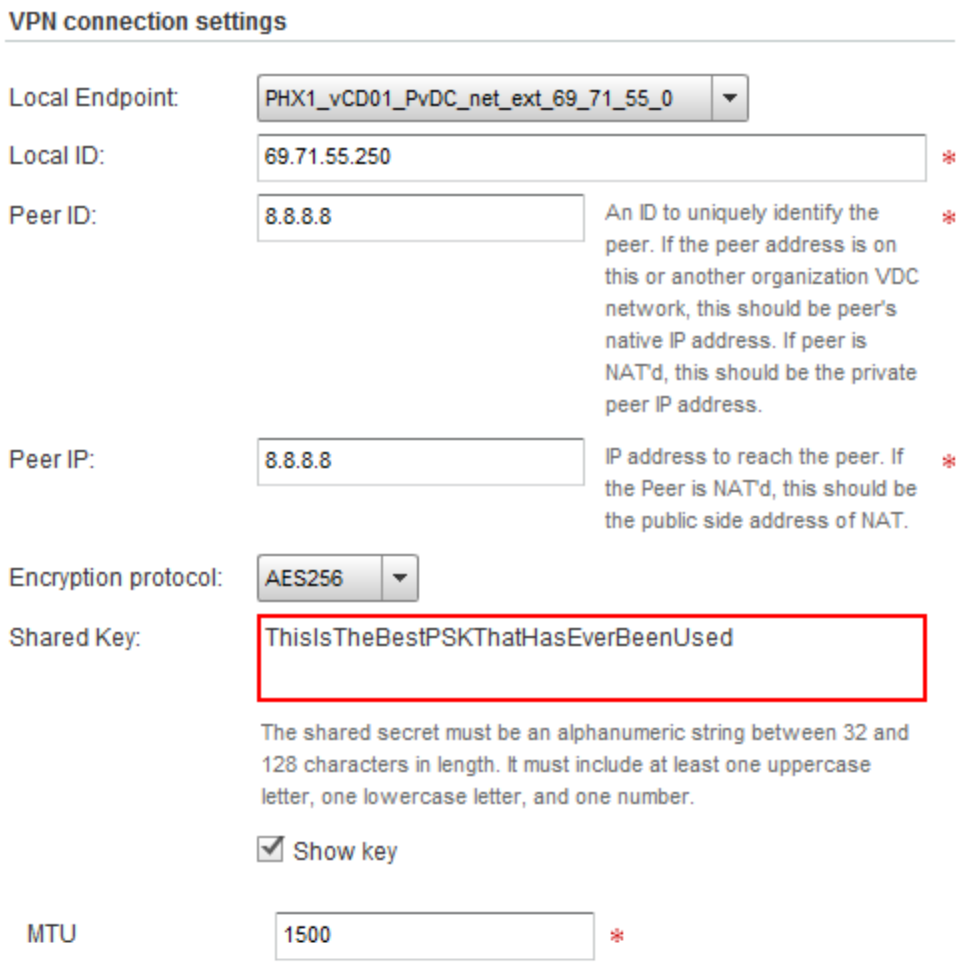


Figure 14 - VPN Configuration 3

Please note that Pre-Shared Keys for VPNs on Edge Gateways must be a minimum of 32 characters in length. Ensure that the MTU size is correct for the remote network device, and the VPN configuration is complete. Select "OK" to complete the configuration.

VPN Firewall Rules

An additional firewall rule will be necessary in order to pass traffic across the VPN. Without this Firewall rule no traffic will be allowed and both endpoints will report the VPN as down.

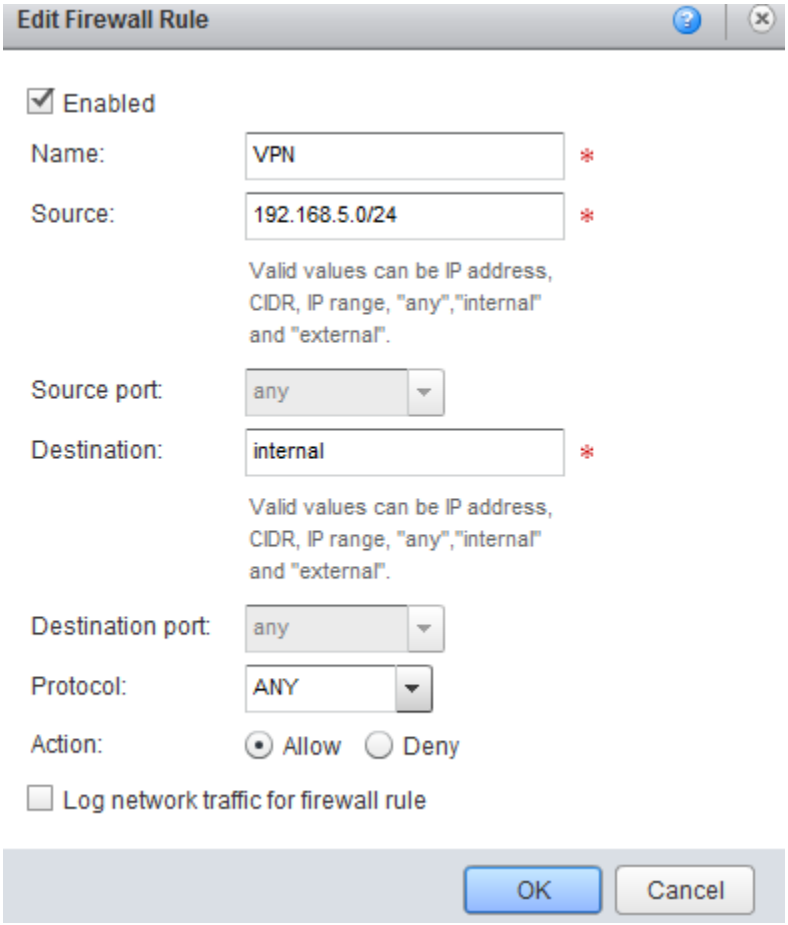


Figure 15 - VPN Firewall Rule

This Firewall rule allows traffic from the remote/peer subnet (see the configuration above) to flow to any internal/private subnet, which includes the internal network on which the client's VMs should be addressed.

At this point the corresponding settings must be entered on the remote network device in order to begin VPN negotiation. Note that the Edge Gateways on vCloud follow the VMware default configuration listed in this KB article. The only exception to this is that Edge Gateways in Nashville, Houston, and Greenville use DH Group 5 rather than Group 2 as specified. Logs and further support may be obtained by contacting GreenCloud Support.

VPN Configuration Settings

Please see below for a list of VMware Edge Gateway default settings for VPNs.

Setting Name	Setting Value
IKE Phase 1	
Encryption	TripleDES/AES, SHA1
Diffie-Hellman Group	MODP Group 2 (1024 Bits)
SA Lifetime	28800 seconds
ISAKMP Aggressive Mode	Disabled
IKE Phase 2	
Encryption	Matches Phase1
Diffie-Hellman Group	MODP Group 2 (1024 Bits)
Perfect Forward Secrecy	Enabled
SA Lifetime	3600 seconds

Appendix A – Revision History

Author	Date	Comments	Ver.
Alex Reid	2017-08-04	Management, NAT, Firewall	
Alex Reid	2017-08-10	VPN, Formatting	0.1
Alex Reid	2017-08-25	VPN Settings Matrix, ICMP Firewall Rule	0.2
Alex Reid	2017-08-30	Initial Publication	1.0