Blue Coat® Systems

Client Manager Redundancy for ProxyClient Deployments

Blue Coat®

CONTROL IS YOURS™

Americas:

Blue Coat Systems, Inc.
420 N. Mary Ave.
Sunnyvale, CA 94085

Rest of the World:

Blue Coat Systems International SARL
3a Route des Arsenaux
1700 Fribourg, Switzerland

Document History

Date	Version	Note
January 15, 2013	v0.1	Initial release

Contents

List of Figures

Introduction

ProxyClient is Blue Coat's remote user solution for WAN Optimization and basic Web Filtering. ProxyClient allows organizations to give remote users access to network resources with LAN-like performance, even when those users are connecting from outside the corporate network, for example, home, customer, or business-partner offices. This access is typically over the Internet using a VPN. ProxyClient can also enforce a per-user Web Filtering policy.

Deployments make use of a ProxyClient Manager, which acts as a central repository for configuration files and software. In most scenarios, the ProxyClient polls the Manager periodically to check for configuration or software version changes. The Manager must therefore be accessible to all deployed ProxyClients. In the case of a large deployment with hundreds of ProxyClients, Manager availability becomes very important.

This document describes how to increase the reliability and scalability of ProxyClient deployments using multiple Client Managers.

Scenario

When a ProxyClient Manager is configured, it creates an installation package that includes the ProxyClient application itself and an associated XML configuration file. The installation package is published on the Manager by default over HTTPS on TCP port 8084, for example: https://ip.address.of.manager:8084/proxyclient/ProxyClientSetup.exe. This URL is configurable, and can be either an IP address or a DNS address; it is included in the XML configuration file so that the ProxyClient has the location of the Manager.

The package can be obtained from this location for installation, and after the ProxyClient is installed and active, it polls the Manager to check for changes. If necessary, it will then download updated software or configuration.

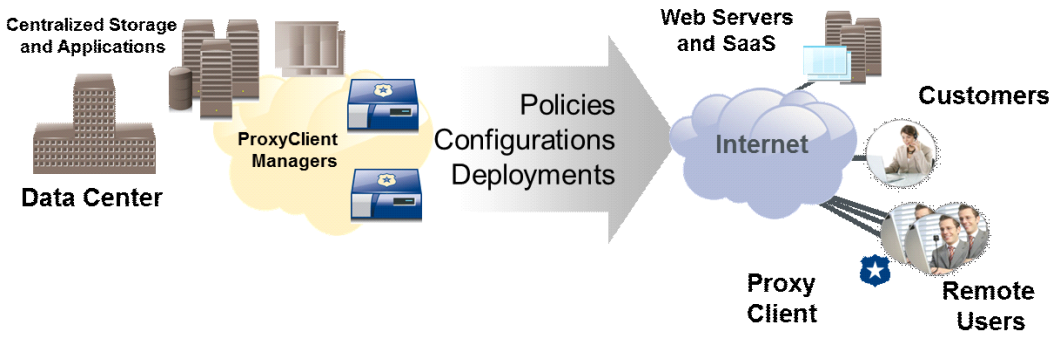

Figure 1–1 Example of a ProxyClient deployment

In a typical scenario, an organization deploying a ProxyClient for WAN Optimization must include a Client Manager at the data center, and make this available on the Internet so that roaming users can always obtain updates from any location. This requires the Client Manager's IP address to be available on the

Internet, most likely with a static NAT address configured on the firewall. Alternatively, the Client Managers can only be made accessible internally, and require VPN connectivity for updates.

For high availability, it is necessary to deploy at least two Client Managers with identical ProxyClient configurations, and some form of load balancing to distribute update requests to each device. These appliances can be located at the same data center or at different data centers, depending on the network architecture. This could also be a good way to achieve scalability for large deployments.

The simplest way to do this is to configure the Client Managers to publish a DNS address based update URL, and then use DNS Round Robin to distribute ProxyClient requests between the Managers.

Alternatively, a hardware load-balancer can be used. In the case of geographically distributed deployments, Global Server Load Balancing can be employed to direct users to Client Managers. The key point in each of these scenarios is that the ProxyClient Managers are accessible through a single DNS name, and the ProxyClient configuration on each Manager is identical.

Requirements

This configuration guide includes the following assumptions:

- The ProxySG appliances that will be used as Managers are already configured and running on the network.
- For ProxyClient acceleration functionality, an ADN should already be configured and an ADN Manager assigned, since an ADN Manager is mandatory for ProxyClient ADN.
- If Web Filtering capabilities are required, then the following requirements must also be met:
  - The device must be licensed as a Full Proxy Edition.
  - Blue Coat Web Filter must be installed on the designated ProxyClient Managers.
  - Blue Coat Web Filter must be licensed for the appropriate number of users.

Refer to the following documents, which are available at:
https://bto.bluecoat.com/

- *ProxyClient Administration and Deployment Guide*
- *SGOS Administration Guide*
- *Acceleration WebGuide*

An ADN Manager can be the same device as a ProxyClient Manager, but dedicated devices should be used if many (for example, hundreds) ProxyClients are envisaged.

There are no specific software requirements, although it is recommended that the latest release of SGOS be used on the Client Managers, whether that version is in the SGOS 5.x or SGOS 6.x code stream. It is also important to use the latest ProxyClient image. All Managers should ideally have the same SGOS and ProxyClient version installed.

For more information on recommended SGOS releases and ProxyClient images, go to https://bto.bluecoat.com/

Configuration Steps

Complete the following procedure to configure the Client Managers.

Procedure:

1. From the ProxySG Management Console, select **Configuration > ProxyClient > General > Client Manager**. (See Figure 1–2.)
2. Select the **Enable Client Manager** check box.
3. Select **Use Host** and specify the client update URL in the field provided. The example is using "client-mgr.company.com."

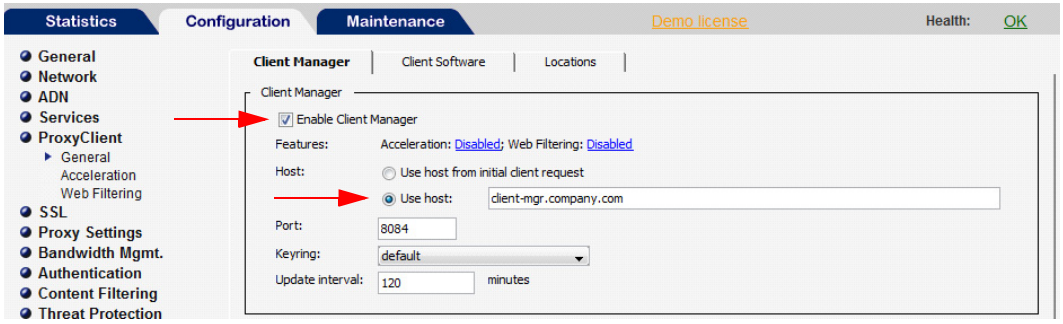

Figure 1–2 Client Manager dialog

4. Click **Apply** to activate changes. The update URL is now reflected in the configuration. (See Figure 1–3.)

Figure 1–3 Update URL

5. If required, define locations and behaviors from the **Locations** tab.
6. (Optional) Enable Acceleration.

a. From the ProxyClient Management Console, select **Configuration > ProxyClient > Acceleration > General**. (See Figure 1–4.)

b. Select the **Enable Acceleration** check box.

c. Specify **Primary** and **Backup ADN Manager IP address**.

d. Click **Apply** to activate changes.

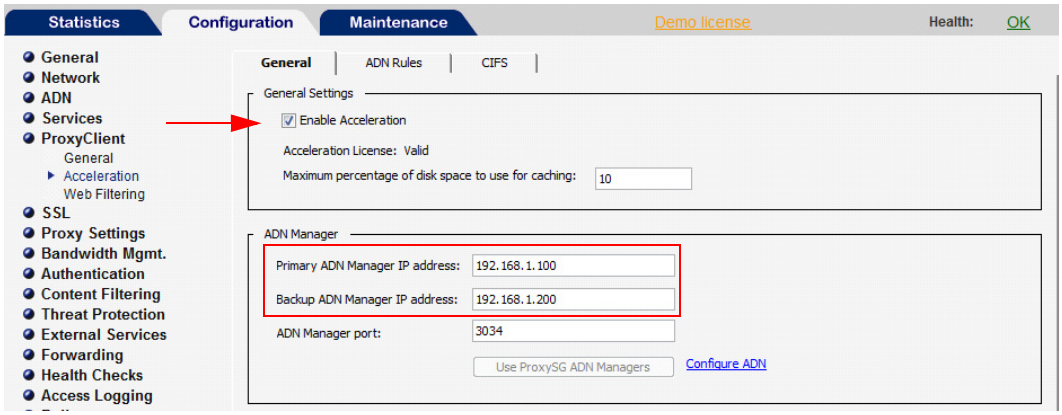

Figure 1–4 Configuration tab - Configuring Acceleration and ADN

7. (Optional) Configure any other parameters from the **ADN Rules** and **CIFS** tabs.

8. (Optional) Enable Web Filtering.

   a. From the ProxyClient Management Console, select **Configuration > ProxyClient > Web Filtering > Policy**. (See Figure 1–5.)

   b. Select the **Enable Web filtering** check box.

   c. Define the Filtering policy.

   d. Click **Apply** to activate changes

   e. Check the **Exceptions** and **Log** tabs, then make any necessary adjustments, as required.

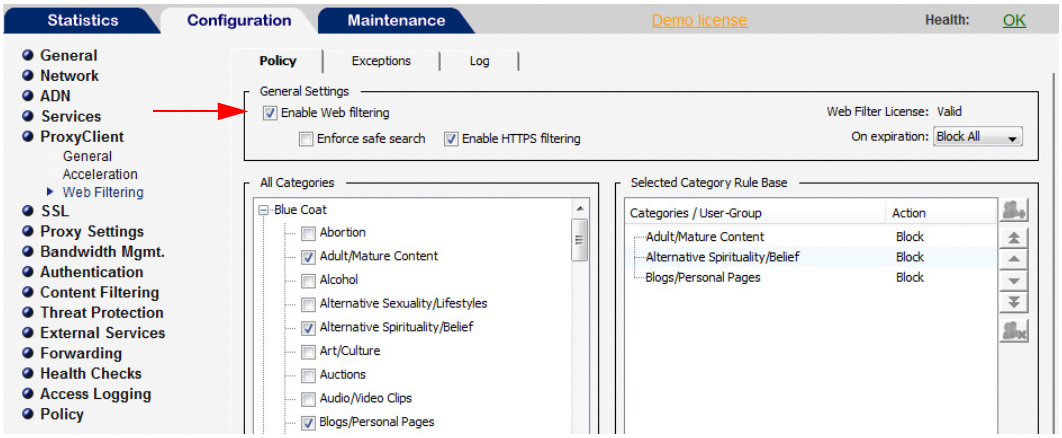

Figure 1–5 Configuration tab - Configuring Web filtering

9. You must repeat steps 1–8 on all other designated Client Managers.
10. Update the externally published DNS zone to reflect the Client Update URL specified in step 3 above.

Note: It is vital that any future ProxyClient configuration changes be replicated across all Managers to ensure consistent behavior. This can be done manually or through the use the Blue Coat Director. Other tools might also be available. For more information, contact your local Blue Coat sales representative.

Advanced Features

DNS Round Robin

DNS Round Robin is a simple way to distribute requests across multiple Managers. One potential issue, however, is that DNS Round Robin doesn't cater to device failures. Therefore, if a Manager become unavailable, DNS won't immediately reflect this. As a result, ProxyClients could make requests to a device that cannot respond.

A workaround is to use the built-in failover capabilities of the ProxySG appliance (SGRP) to share Virtual IP addresses among devices. Thus, a device has a primary address that is referenced in DNS that acts as a backup for any secondary addresses. If a device fails, its primary address automatically becomes available on another device, thus providing seamless failover from a ProxyClient perspective. This can be useful in providing continuous service temporarily until the failed device is brought back online.

For more information, refer to the following:

- See "Configuring DNS Round Robin" on page 6 for a sample configuration.
- Go to https://kb.bluecoat.com for information on configuring failover and its suitability when used with different applications.

Conclusion

Client Managers perform a vital role in enabling functionality for remote users, and when robust and scalable deployments are desirable. DNS Round Robin is a simple way to achieve this high availability, and is straightforward to configure. Additional resilience can be provided by configuring ProxySG appliance Failover. Alternatives to DNS Round Robin are Global Server Load Balancing and Hardware Load Balancers.

Appendix

Configuring DNS Round Robin

DNS Round Robin requires that each relevant Client Manager IP address be configured against the same DNS A-Record. In this case, each request for the Client Update URL would resolve to the different IP addresses in sequence, thus distributing requests across the various Client Managers. For example:

```
; Client Manager definitions for ProxyClient
client-mgr    IN  A           192.168.0.1  ; mgr1
              IN  A           192.168.0.2  ; mgr2
              IN  A           192.168.0.3  ; mgr3
```

About Technical Briefs

Technical briefs are designed to illustrate the features and capabilities of Blue Coat products. By describing generic solutions, technical briefs provide a foundation that Blue Coat customers can use to understand how Blue Coat products can be used to solve specific problems.

These technical briefs are not intended to solve customer-specific requests; if you need a customized solution to address a specific concern, contact Blue Coat Professional Services at Professional.Services@bluecoat.com.