Blue Coat® Systems

Connecting the ProxySG Appliance to Blue Coat Support Systems and Cloud Central Appliance Monitoring in Closed Networks

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

Introduction 1
Explanation of Services and Destinations 1
Scenarios 2
Requirements 2
Configuration 2
    Configuring Mach5 Devices 2
    Configuring VPM 4
    CPL code 8
    Configuring the Internet Proxy Devices 8
Verification Testing 10
    Verifying Heartbeat 10
    Verifying PDM Export (Appliance Monitoring in the Cloud) 11
Conclusion 12
About Technical Briefs 13

List of Figures

Example scenario 2
Add Forwarding Host dialog 3
Health Checks tab 4
Visual Policy Manager main page 4
Add Combined Destination Object dialog 5
Add Combined Destination Object dialog 6
Add Select Forwarding Object dialog 7
New Forwarding Layer policy rule 7
Sample Web Application Layer rule 9
Sample Web Authentication Layer rule 9
ThreatPulse main page 11

Introduction

Having WAN Optimization devices (for example, ProxySG Mach5 edition) installed in private/closed network environments (for example, MPLS networks) prevents the use from accessing three helpful features on the ProxySG appliance:

- Sending service information to Blue Coat Support directly from the ProxySG appliance User Interface
- Participation in Blue Coat´s Customer Experience Program (also called Heartbeat)
- Using Appliance Monitoring in the Cloud

The following guide shows how to leverage an existing Internet Proxy (a ProxySG appliance is used in this example) to connect Mach5 devices to the Internet and allow them to use the features mentioned above. At the same time, no direct Internet access is necessary, which allows more granular control over this kind of traffic and avoids breaking the security policy of many companies.

Explanation of Services and Destinations

- For sending service information, the following URL is used: upload.bluecoat.com
- For sending heartbeat information, the following URL is used: hb.bluecoat.com
- For sending PDM Statistics to the Cloud, the URL used is unique to your Blue Coat ThreatPulse service account. The common part of this URLis: stats.threatpulse.com/pdm/config/
- The information is encrypted and transferred to Blue Coat using HTTPS.
- More background on how to use these features can be found in the *SGOS Administration Guide*.
- These three URLs will be accessed by the Mach5 device.

Scenarios

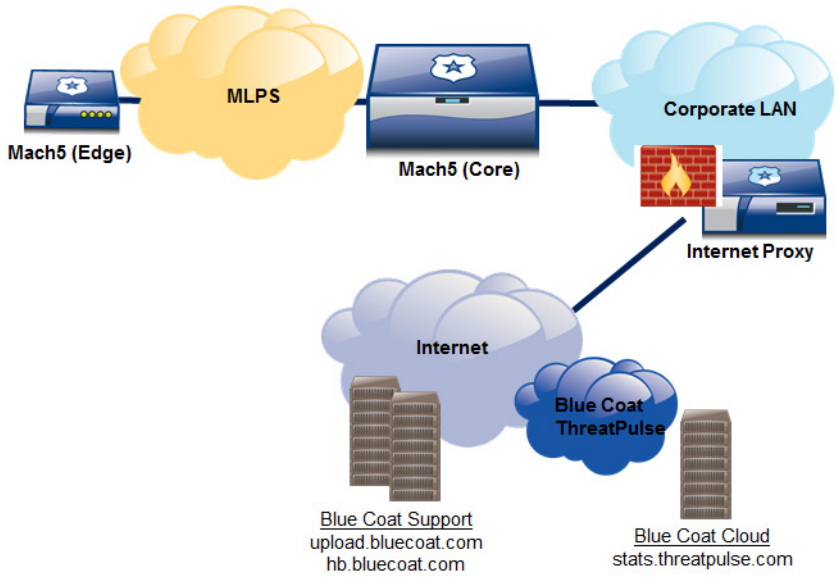

Figure 1–1 Example scenario

Requirements

You need to know the IP address or URL of the Internet proxy and the port on which this proxy is listening. Furthermore, the Mach5 devices need connectivity to the Proxy.

Note: The Mach5 devices do not need direct access to the Internet.

Configuration

Configuring Mach5 Devices

To allow the Mach5 devices that are located in the closed part of the network to connect to Blue Coat´s Support and Monitoring systems, you need to configure a forwarding host and a forwarding policy.

Procedure:

In this procedure, you will configure a Forwarding Host. (See Figure 1–2.)

1. From the ProxySG Management Console, select **Configuration > Forwarding > Forwarding Hosts.**
2. Click **New.**

   The **Add Forwarding Host** dialog displays.

3. Create a new Forwarding Host using the following parameters:

   Alias = The nickname of your Internet Proxy

   Host = The Internet Proxy resolvable hostname or IP address

   Type = **Proxy**

   Port = Listener port on your Internet Proxy (for example, 8080 or 3128)

4. Click **OK**.

   The dialog closes.

5. Click **Apply**.

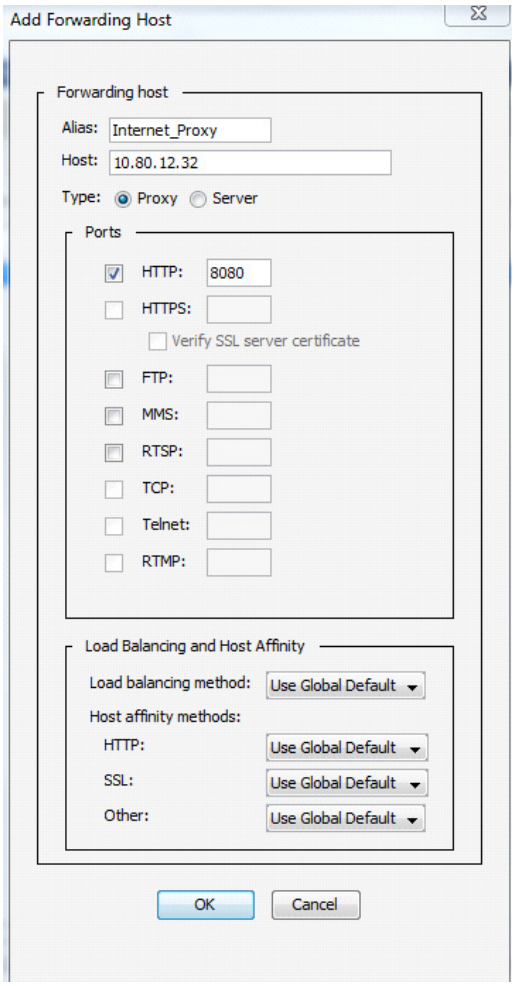

Figure 1–2 Add Forwarding Host dialog

6. Verify Health Check.

   a. From the ProxySG Management Console, select **Statistics > Health Checks**. (See Figure 1–3.)

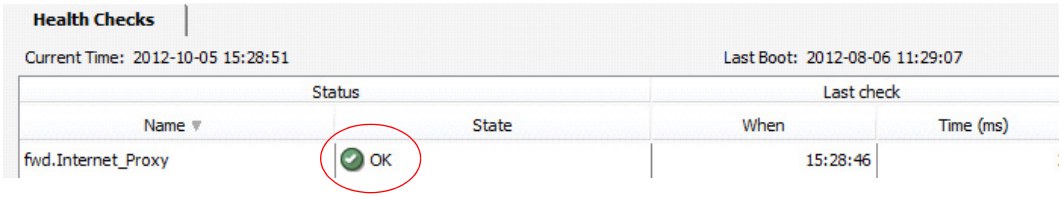

Figure 1–3 Health Checks tab

When configuring the Forwarding Hosts, the system automatically generates a health check entry, which verifies if the Forwarding Host is reachable, available, and listening on the specified port.

a. Ensure that the Health Check of the Forwarding Host shows **OK**.

If the health check state is not OK, check the following:

- Connectivity
- Routing
- DNS resolution

7. Configure Forwarding Policy.

   To tell the Mach5 devices to use the Internet proxy for the above-mentioned URLs (upload.bluecoat.com, hb.bluecoat.com, and stats.threatpulse.com/pdm/config) a forwarding policy must be configured. This can be done in CPL (for example, local policy), or using the graphical Visual Policy Manager (VPM). For more information, see "Configuring VPM".

Configuring VPM

The following procedure describes how to configure the ProxySG appliance using VPM and also shows the CPL for reference. Using this procedure, you will add a new Forwarding Layer and change the destination.

1. From the ProxySG Management Console, select **Configuration > Policy > Visual Policy Manager.**
2. Click **Launch** to launch VPM. (See Figure 1–4.)

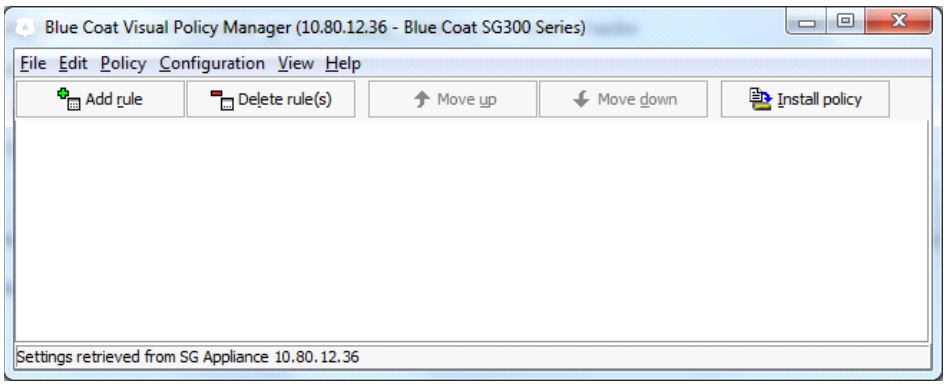

Figure 1–4 Visual Policy Manager main page

3. From the **Policy** menu, select **Add Forwarding Layer.**
4. On the created rule, right-click the **Destination** column and select **Set.**
5. Click **New,** then select **Combined Destination Object.**

   The **Add Combined Destination Object** dialog displays. (See Figure 1–5.)

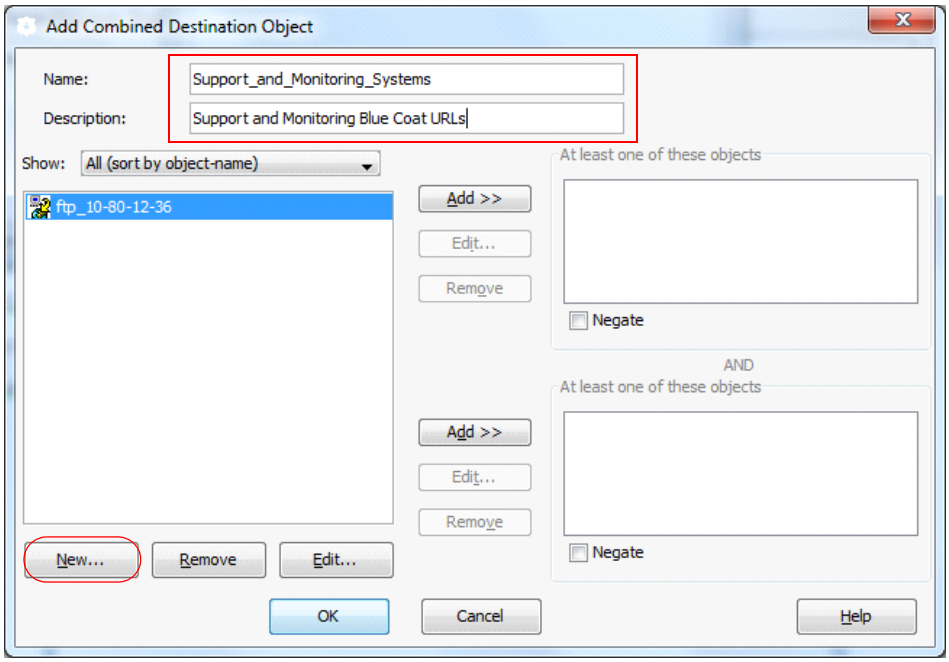

Figure 1–5 Add Combined Destination Object dialog

6. Enter a comprehensive name for the object. The example is using "Support_and_Monitoring_Systems."
7. Enter a description for the object. The example is using "Support and Monitoring Blue Coat URLs."
8. Click **New,** then select **Server URL.**
9. Enter **upload.bluecoat.com** in the URL field.
10. Repeat steps 8 and 9 with the following URLs:

    hb.bluecoat.com

    stats.threatpulse.com/pdm/config/
11. Select the three Server URL objects you just created, then click **Add >>** to add them to the upper right **At least one of these objects** window. (See Figure 1–6.)

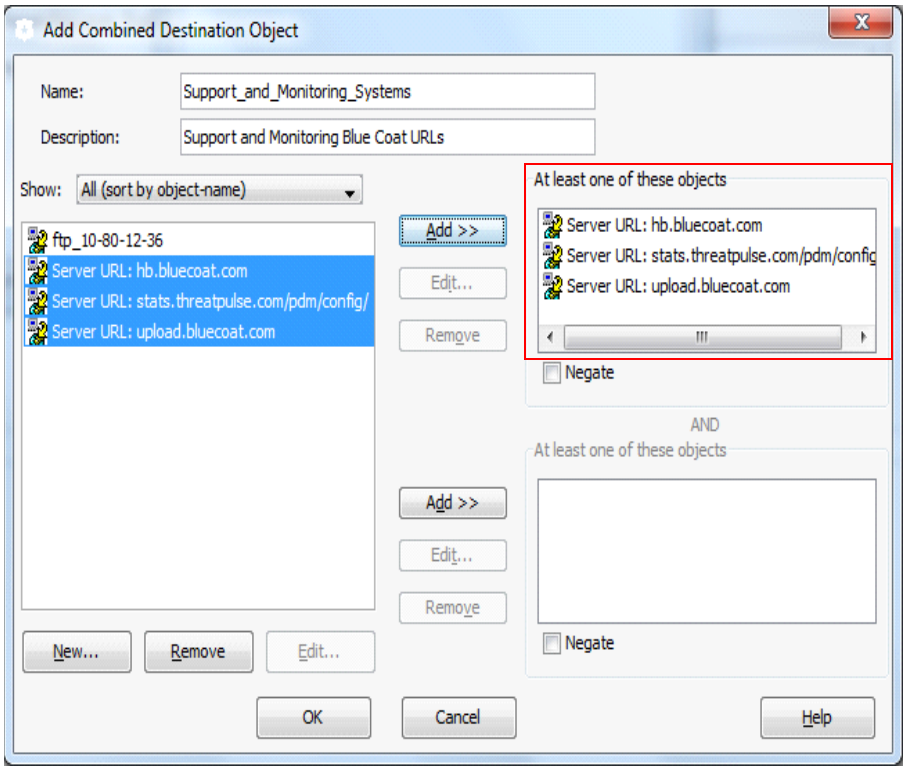

Figure 1–6 Add Combined Destination Object dialog

12. Click **OK**.

    The dialog closes and you return to the VPM main page.

13. On the created rule, right-click the **Action** column and select **Set**.
14. Click **New**, then select **Select Forwarding Object**.
15. Enter a comprehensive name for the object.
16. Select the newly created **Forwarding Host** from the list and click **Add >>** to add it to the right window. (See Figure 1–7.)

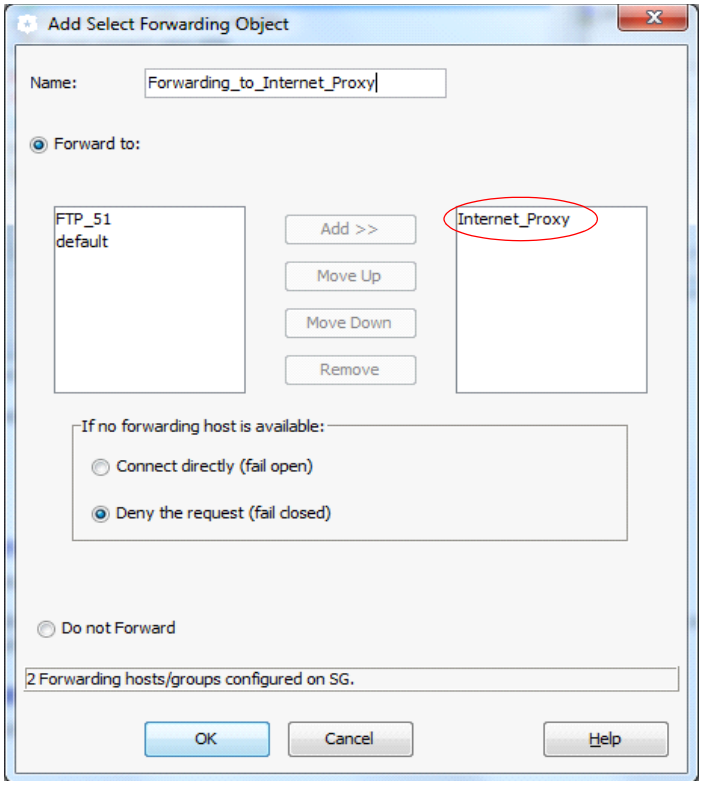

Figure 1–7 Add Select Forwarding Object dialog

17. Click **OK**.

    The dialog closes and you return to the **Add Combined Destination Object** dialog.

18. Click **OK**.

    The dialog closes and you return to the VPM main page. The new rule is listed in the table. (See Figure 1–8.)

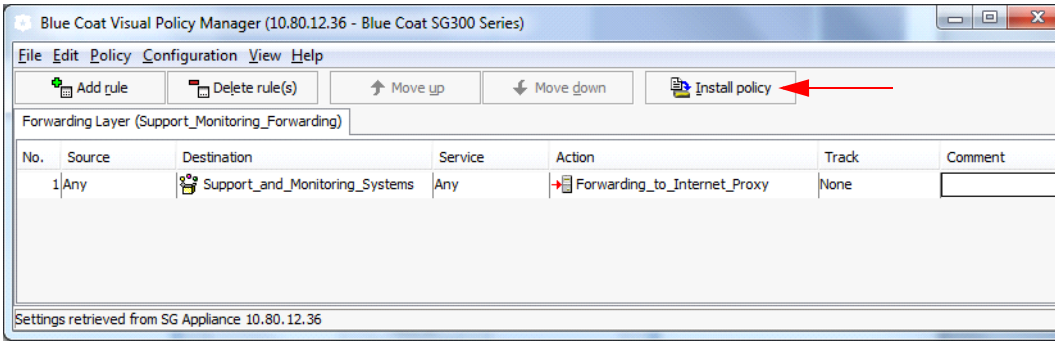

Figure 1–8 New Forwarding Layer policy rule

19. Click **Install policy**.

To view the equivalent generated CPL code for the rule you just created, see "CPL code" on page 8.

CPL code

```
;; Description: Support and Monitoring Blue Coat URLs
define condition __CondList1Support_and_Monitoring_Systems
        server_url.domain="hb.bluecoat.com"
        server_url.domain="stats.threatpulse.com/pdm/config/"
        server_url.domain="upload.bluecoat.com"
end condition __CondList1Support_and_Monitoring_Systems

define condition Support_and_Monitoring_Systems
        condition=__CondList1Support_and_Monitoring_Systems
end condition Support_and_Monitoring_Systems


;; Tab: [Forwarding Layer (Support_Monitoring_Forwarding)]
<Forward>
        condition=Support_and_Monitoring_Systems
forward("Internet_Proxy") forward.fail_open(no)
```

Note: You can use the above CPL and import it to your local policy file.

Configuring the Internet Proxy Devices

The Internet proxy gets the forwarded requests from the Mach5 devices. Depending on the existing policy for authentication and content, these requests might be denied.

The Mach5 devices cannot authenticate themselves to the Internet proxy. As a result, you need to make sure that the Internet proxy:

- Listens on the port used for forwarding on the Mach5 devices. (In the above example, the port is 8080.)
- Does not require a user authentication from the Mach5 devices.
- Allows the requests to hb.bluecoat.com, upload.bluecoat.com and stats.threatpulse.com/pdm/config/.

The following is a policy example on a ProxySG appliance acting as the Internet proxy:

1. Adapt the **Web Authentication Layer** to not require user authentication for the three destination URLs.
2. As described previously, create a similar **Combined Destination Object** that includes the three Support and Monitor URLs.
3. Create a rule similar to the one shown in Figure 1–9.

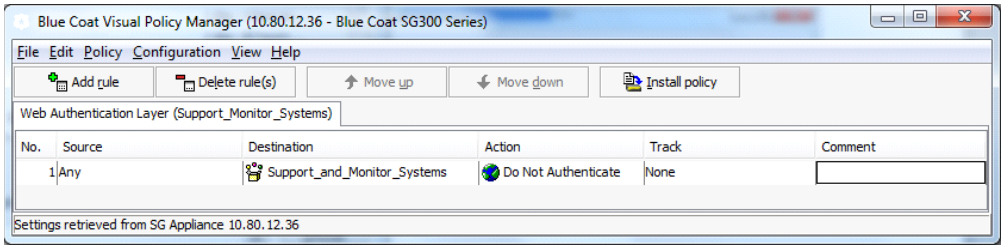

Figure 1–9 Sample Web Application Layer rule

4. Adapt the **Web Access Layer** to allow access to the three destination URLs.
5. Create a rule similar to the one shown in Figure 1–10.

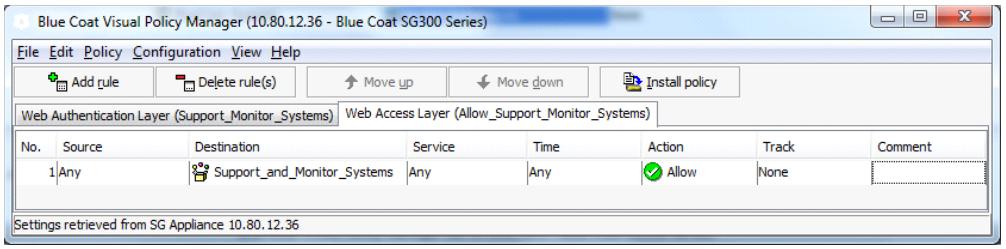

Figure 1–10 Sample Web Authentication Layer rule

Optionally, you can restrict these two rules with a source object specifying the source IP addresses of all Mach5 devices on the network.

The CPL Policy looks like the following example:

```
;; Description:
define condition __CondList1Support_and_Monitor_Systems
        url.domain="toto.fr"
end condition __CondList1Support_and_Monitor_Systems

define condition Support_and_Monitor_Systems
        condition=__CondList1Support_and_Monitor_Systems
end condition Support_and_Monitor_Systems



;; Tab: [Web Authentication Layer (Support_Monitor_Systems)]
<Proxy>
        condition=Support_and_Monitor_Systems authenticate(no)

;; Tab: [Web Access Layer (Allow_Support_Monitor_Systems)]
<Proxy>
        condition=Support_and_Monitor_Systems Allow
```

Verification Testing

Verifying Heartbeat

For testing purposes, you can manually trigger a heartbeat and simultaneously monitor the access log on the Internet proxy.

To trigger a manual heartbeat from a Mach5 device, from the CLI console, complete the following procedure.

Procedure:

1. Log in to the device.
2. Go to **enable** mode.

```
SG> enable
Enable Password:
```

3. Go to **conf t** mode.

```
SG# conf t
Enter configuration commands, one per line.  End with CTRL-Z.
```

4. Go to **diagnostics**.

```
SG# (config)diagnostics
```

5. Enter the command **send-heartbeat**.

```
SG# (config diagnostics)send-heartbeat
  ok
SG# (config diagnostics)
```

If you check the access log on the Internet proxy, you should see the forwarded and allowed request:

```
#Start-Date: 2012-10-05 14:23:05 #Date: 2011-08-17 06:02:51
#Fields: date time time-taken c-ip cs-username cs-auth-group x-
exception-id sc-filter-result cs-categories cs(Referer) sc-status s-
action cs-method rs(Content-Type) cs-uri-scheme cs-host cs-uri-port
cs-uri-path cs-uri-query cs-uri-extension cs(User-Agent) s-ip sc-bytes
cs-bytes x-virus-id
#Remark: 1206060036

2012-10-05 14:23:11 44 10.10.10.254 - - - PROXIED "Computers/Internet"
-  200 TCP_ACCELERATED CONNECT - tcp hb.bluecoat.com 443 / - -
"Mozilla/4.0 (compatible;)" 20.20.20.254 39 102 -
```

Verifying PDM Export (Appliance Monitoring in the Cloud)

To enable and verify this feature, certain requirements must be met:

- A valid ThreatPulse account is needed to collect PDM exported data.

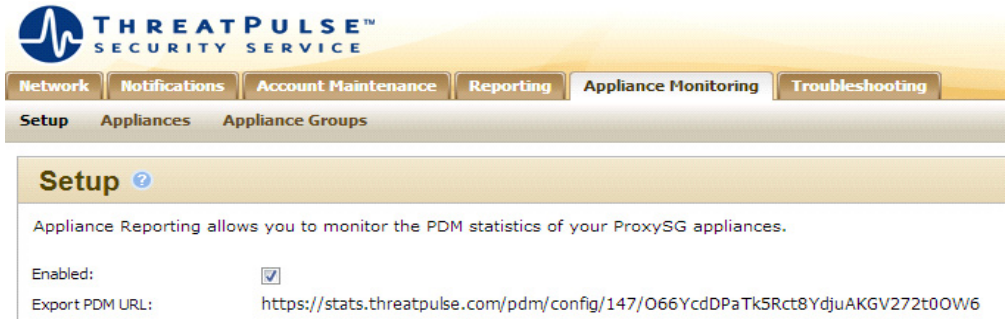

Figure 1–11 ThreatPulse main page

- The PDM export feature must be enabled on the Mach5 devices.

```
10.80.12.36 - Blue Coat SG300 Series#(config statistics-export)config-
path https://stats.threatpulse.com/pdm/config/147/
O66YcdDPaTk5Rct8YdjuAKGV272t0OW6
  ok
```

- The configured URL must be the one shown on the ThreatPulse portal (see above).

```
10.80.12.36 - Blue Coat SG300 Series#(config statistics-export)enable
  ok
```

To verify that PDM export is working, complete the following procedure.

Procedure:

1. Go to the Mach5 device CLI console.
2. Log in.
3. Go to **enable** mode.

```
SG> enable
Enable Password:
```

4. Go to **conf t** mode.

```
SG# conf t
Enter configuration commands, one per line.  End with CTRL-Z.
```

5. Go to **statistics-export**.

```
SG# (config)statistics-export
```

6. Enter the command **force-export** (to force PDM export).

```
10.80.12.36 - Blue Coat SG300 Series# (config statistics-export)force-
export
Next data export will happen in 58 seconds.
```

7. Validate the export process using the **view** command.

```
10.80.12.36 - Blue Coat SG300 Series#(config statistics-export)view
Statistics export configuration
  Statistics export:                Enabled
  Configuration path:               https://stats.threatpulse.com/pdm/
config/147/O66YcdDPaTk5Rct8YdjuAKGV272t0OW6
  SSL device profile:               default
  Configuration information:
    Details of last configuration download:
       Configuration path:          https://stats.threatpulse.com/pdm/
config/147/O66YcdDPaTk5Rct8YdjuAKGV272t0OW6?version=1-
1&sn=1311165028&ip=10.80.12.36&model=300-25
        Last attempted config:      2012-10-05 14:29:52 UTC
        Last successful config:     2012-10-05 14:29:52 UTC
    Details of active configuration:
        Version:                    1
        Time interval:              15 minutes
        Trend filter:
        Upload path:                https://stats.threatpulse.com/pdm/
upload/147/O66YcdDPaTk5Rct8YdjuAKGV272t0OW6


  Upload information:
    Details of last upload:
       Upload path:                 https://stats.threatpulse.com/pdm/
upload/147/O66YcdDPaTk5Rct8YdjuAKGV272t0OW6
        Last attempted upload time: 2012-10-05 14:30:03 UTC
        Last successful upload time: 2012-10-05 14:30:03 UTC
    Next estimated upload time:     2012-10-05 14:46:42 UTC
    Successful uploads:             1
    Failed upload attempts:         0
    Data lost in minutes:           0
```

Conclusion

This document provides a step-by-step guide for connecting ProxySG appliances that are deployed in a closed network environment without secure, direct Internet access to the outside world. By following the easy-to-follow outlined steps, customers can leverage Blue Coat´s support systems and directly upload troubleshooting information to support service requests and thereby ease the support process. Furthermore, the document explains how to connect ProxySG appliances to Blue Coat´s ThreatPulse system for using the Central Appliance Monitoring feature – a powerful feature to monitor a distributed deployment.

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.