



Executive Summary

As the leader in Wide Area Application Delivery, Blue Coat products accelerate and secure applications within your WAN and across the Internet. Blue Coat provides a robust and flexible solution that controls users and network resources, protects against Web-based threats, and accelerates the broadest range of WAN-based applications. Whether deployed on either end of a WAN, at Internet access points, or in front of business-critical services, Blue Coat ProxySG appliances provide control points that stop the bad and accelerate the good. At the heart of this solution is the Blue Coat Policy Processing Engine which allows administrators to apply policy-based control over user requests, providing them with complete control over how data in the path of the proxy is processed.

What is the Blue Coat Policy Processing Engine?

The Blue Coat Policy Processing Engine provides a flexible, comprehensive policy architecture that allows administrators to control data communications across users, content types, applications, and security services. Because of its powerful policy enforcement abilities, the Blue Coat Policy Processing Engine is the core of a ProxySG appliance configuration. The Policy Processing Engine makes decisions about how to process traffic passing through the appliance, allowing administrators to create granular security and performance policies related to who, what, where, when, and how individual users and applications communicate internally and externally. The Blue Coat Policy Processing Engine is controlled by both the Visual Policy Manager (VPM) and a syntax known as Content Policy Language (CPL).

Why should I use the Blue Coat Policy Processing Engine?

Although there are various policy and control options available to administrators, there are several advantages to using the Blue Coat Policy Processing Engine instead of enforcing policy elsewhere in the network. First and foremost is visibility. Because the ProxySG appliance is often deployed in the path of traffic, with visibility to all traffic on the wire, it is the ideal place in the network to provide policy-based control. The ProxySG's native understanding of application layer information further differentiates the level of visibility available with Blue Coat ProxySG appliances, allowing the Blue Coat Policy Processing Engine to provide a far richer framework for controlling and monitoring the user-application pairing than packet delivery devices. This is especially true for SSL-encrypted content, since other devices on the network lack visibility into the actual content obfuscated by SSL; ProxySG appliances can open and inspect SSL content. Another key benefit of enforcing network policy on the ProxySG appliance is the flexibility and breadth of policy control available. The Blue Coat Policy Processing Engine is designed to provide administrators with a comprehensive tool for enforcing the unique policies required by the enterprise. These policies may be associated with local regulatory compliance or with policies defined by the administrator to ensure that business-critical applications always receive priority over all other traffic. Regardless of the policy to be implemented, the Blue Coat Policy Processing Engine is the comprehensive tool of choice, with an extensive list of available policy options to create an almost limitless combination of rules.



How does the Blue Coat Policy Processing Engine work?

Blue Coat Policy Processing Engine policy enforcement is based on policies configured by the network administrator using either the VPM or CPL. All Blue Coat ProxySG appliances start with a default policy rule, to implicitly allow or implicitly deny traffic, which should be set based on preferred security posture; additional policy rules are determined by the role(s) of the appliance in the network. If the administrator has configured a default rule of allow, the policy reflects a corporate security policy to “allow everything except...”. If the default is set to deny, the policy reflects a corporate security policy of “deny everything except...”.

Policy Creation

Blue Coat ProxySG appliances support two methods of creating policy--VPM and CPL. The Visual Policy Manager (VPM) is a user-friendly graphical interface located in the ProxySG Management Console which allows administrators to create policy using simple pull-down menus and checkboxes. More advanced users can choose to use Content Policy Language (CPL) to write policy. A combination of both is also common.

Policy Evaluation

Policy is based on the concept of layers and rules. A policy layer is a construct with several purposes. First, it serves to separate rules for unrelated decisions. For example, administrative policy is done in the <admin> layer, whereas forwarding (upstream routing) is handled by the <forward> layer. Another function of layers is to serve as a set of rules that when evaluated result in one policy decision being reached. A layer and its embedded rules can be viewed as one cascading “if..then..else..if” statement. Separating decisions helps facilitate policy cohesion and limits complexity. Another function of layers is to refine decisions reached in previous layers. An early layer may establish general policy which can be later refined in subsequent layers. Using this same concept, later layers can also override decisions reached in earlier layers.

A policy rule consists of one or more conditions and some number of property settings. When a rule is evaluated, the conditions are tested for that particular transaction. If all of the conditions evaluate to true, the rule is said to match. On a match, all of the listed property settings are executed (though later layers can potentially override the action) and evaluation of the current layer ends. If one or more of the the conditions evaluate to false for that transaction, it is said to be a miss, and policy evaluation continues to the next rule in the layer.

```
<layer 1>
  rule 1
  rule 2
  rule 3

<layer 2>
  rule 1
  rule 2
```



Policy Example 1a

An administrator who has configured a default policy of allow would like to block access to sports and gambling sites for all employees during business hours. The logical form of the policy rule could be expressed as: "If the destination is a sports or gambling site AND the time is between 9am and 5pm, deny the request." The actual syntax would be as follows:

```
<proxy>  
  category=(sports, gambling) time=0900..1700 DENY
```

Policy Example 1b

The CEO was not happy to find that he could not access his favorite sports site to check scores during business hours. The administrator therefore added a new rule allowing the CEO to access sports sites with no time restriction. This rule is placed before the current rule since the first rule to match in the layer will prevent the evaluation of further rules in the layer. The logical form of the policy rule could be expressed as: "If the destination is a sports site AND the user is the CEO allow the request, else if the destination is a sports or gambling site AND the time is between 9 a.m. and 5 p.m., deny the request." The actual syntax would be as follows:

```
<proxy>  
  category=(sports) user="CEO" ALLOW  
  category=(sports, gambling) time=0900..1700 DENY
```

Blue Coat Difference

Enhanced Visibility and Control

Many solutions available today allow for extremely localized policies. Unfortunately, this approach restricts the set of decision criteria to the information that can be determined by the local subsystem making the decision. Blue Coat's Policy Processing Engine architecture, however, accumulates information about the request/response interaction from each subsystem involved in the processing, and any of this accumulated information can be tested to reach a decision. This presents a much broader and flexible set of controls, largely isolating the policy author from the variations between protocols. For example, the same high-level authentication rule can be enforced by a variety of protocols, including (through various surrogate credentials) protocols that do not necessarily support authentication.

Policy-Based Control Over Secure Content

With secure (https-enabled) Web applications on the rise, controlling this traffic has become a priority for security-conscious enterprises; lack of control over secure content gives users a means to bypass corporate policies in place and exposes organizations to costly risks. The unique ability of Blue Coat appliances to apply policy-based control over both internal and external SSL applications means that administrators are no longer forced to allow all secure traffic. Instead, administrators can exercise the same level of control over secure traffic as other Web applications on the network with confidence.