INTRODUCTION
Outlook Web App (OWA) offers simple and convenient access to corporate email accounts by using a Web browser on any system from any Internet-connected location. ActiveSync allows users to connect to their corporate email accounts with their smart phones like iOS, Android or Windows Mobile based devices.

Web access from any location, however, introduces security issues such as maintaining information confidentiality, avoiding improper logoffs, removing content left in memory, and providing secure authentication. OWA also places a burden on the server side by using several MB of memory per user to serve up Web-based email, not to mention the overhead generated by encrypted traffic.

The Blue Coat ProxySG serves as the basis for a robust and flexible solution to front-end Microsoft’s OWA (incl. ActiveSync) product and provides the necessary security needed by today’s enterprises. In addition to Web policy management, content filtering, malware-scanning and network protection, companies can implement a scalable and secured Outlook Web App and ActiveSync service using the ProxySG. The ProxySG solution offers encryption of data along with an automatic inactivity timeout enabling administrators to more fully secure access from public networks. This Technical Brief describes how to implement a secure solution for Outlook Web App and ActiveSync using the ProxySG to intercept email traffic before it reaches the mail server.
# Table of Contents

**Introduction**

1

**Implementing Secured Outlook Web App and ActiveSync**

3

**Feature Compatibility Overview**

3

**Basic Reverse Proxy Configuration**

3

  - Configuring the SSL Keyring, Certificate and Reverse Proxy Service
  - Configuring the Forwarding Host
  - Configuring the Forwarding Policy
  - Configuring an external OWA URL on the Exchange Server
  - Configuring an external ActiveSync URL on the Exchange Server
  - Configuring “HTTP to HTTPS” and “/” to “/owa” redirect Policies

3

**Advanced Features**

11

  - IWA (basic) or LDAP authentication with credential forwarding
  - *Enable IWA authentication at the reverse proxy*
  - *Reconfigure OWA to require basic authentication instead of forms based authentication*
  - *Single Sign On Policy (credential forwarding) on ProxySG - OWA*
  - *User Experience*
  - *Single Sign On Policy (credential forwarding) on ProxySG – ActiveSync*

11

- Kerberos Constrained Delegation for OWA
  - *Reconfigure OWA to require IWA authentication*
  - *Verify that IIS supports the “Negotiate” authentication method*
  - *Register SPN*
  - *Configure Delegation for the ProxySG Computer Object*

16

- Single Sign On Policy (KCD) on ProxySG
  - *User Experience*
  - *Verify that the user has been authenticated using KCD*

19

**Conclusion**

20
Implementing Secured Outlook Web App and ActiveSync

There are several options for securing Outlook Web App using the ProxySG:

- Basic reverse proxy features
  - HTTPS termination on the ProxySG
  - Configure an “external URL” on the Exchange Server for OWA and ActiveSync access
  - Redirect HTTP requests to HTTPS and redirect “/” requests to “/owa” (for OWA)

- Advanced features
  - IWA (basic) or LDAP authentication with credential forwarding to achieve a single sign on experience
  - Kerberos Constrained Delegation to achieve a single sign on experience

- Software used for this Tech Brief:
  - SGOS 6.3.1.1 (SGOS 6.5.1.1 for Kerberos Constrained Delegation)
  - Exchange 2010 on Windows Server 2008 R2 SP1
  - MS AD on Windows Server 2008 R2 SP1
  - MS CA on Windows Server 2008 R2 SP1

The following diagram represents the solution for securing Outlook Web App using the Blue Coat ProxySG.

NOTE: In the following examples, the URL “webmail.training.bluecoat.com” is used as the external OWA and ActiveSync URL, and tee-exchange.training.bluecoat.com is used as the OWA server’s internal URL. As you do the procedures, use your own external and internal OWA URLs. This procedure assumes a DNS-based reverse proxy setup, where the hostname, “webmail.training.bluecoat.com” in the procedures, resolves to an externally reachable IP address on the reverse proxy.

We do not cover the inactivity timeout configurations in this document. These are standard features of authentication realms on ProxySG as well as OWA. In short: when using authentication on the ProxySG, you could use inactivity timeout settings on the ProxySG. Otherwise we would recommend using the OWA inactivity timeout settings (for example: http://www.msexchange.org/articles_tutorials/exchange-server-2007/security-message-hygiene/outlook-web-access-security-features-part2.html)

Feature Compatibility Overview

This Technical Brief covers features, which are not applicable for all use cases of OWA and Active Sync. The following matrix provides an overview about the available features and by which application they can be used.

<table>
<thead>
<tr>
<th>FEATURE / CLIENT APPLICATION</th>
<th>OWA SSO (CREDENTIAL FORWARDING)</th>
<th>OWA SSO (KCD)</th>
<th>ACTIVE-SYNC</th>
<th>OUTLOOK ANYWHERE</th>
</tr>
</thead>
<tbody>
<tr>
<td>BROWSER</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>OUTLOOK (THIS HAS NOT BEEN TESTED)</td>
<td>(X)</td>
<td>(X)</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>MOBILE BROWSER</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>ACTIVESYNC CLIENT</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

Outlook Anywhere has not been tested for this Technical Brief. In theory credential forwarding and Kerberos Constrained Delegation should work, however this has to be tested before there are any commitments made.

Basic Reverse Proxy Configuration

Configuring the SSL Keyring, Certificate and Reverse Proxy Service

1. Open the Blue Coat management console on the ProxySG and go to Configuration > SSL > Keyrings as shown to the right.
2. Click Create; the Create Keyring dialog displays.
In this example the keyring is named “OWA” (refer to the manuals for “private key visibility” options). Click OK to create the keyring and dismiss the dialog. Click Apply in the management console. Click OK to dismiss the confirmation dialog.

**NOTE:** If you are going to import a certificate in the next step, then import the keyring for the certificate in this step.

3. Next, create or import a certificate for the new keyring. To do this, select the new keyring and click **Edit/View**.

**NOTE:** A self-signed certificate can be used (which may cause warnings in the browser) or a request can be made with the **Certificate Signing Request** option to a valid CA authority that will then return a signed certificate understood by most browsers. This example creates a self-signed certificate.

4. Click **Create** in the **Certificate** area and fill in the form. Alternatively, if you want to use a CA certificate and have a signed certificate that you can import into the ProxySG, click **Create** in the **Certificate Signing Request** area instead.

**Note:** The **Common Name** option is the URL of the OWA that users enter. This example uses webmail.training.bluecoat.com.

Click **OK** to finish. The dialog goes away and your data is displayed; example follows.

5. To view the certificate, click **View Certificate**, the certificate displays; example follows.

6. Next, the keyring must be assigned to an HTTPS Reverse Proxy service on the ProxySG: From the Blue Coat management console go to **Configuration > Services > Proxy Services** as shown below:

7. Click on **New Service** to create a new HTTPS Reverse Proxy Service. Select HTTPS Reverse Proxy from the **Proxy** dropdown menu to display additional options. Select the previously defined certificate for the **Keyring** option (OWA in the example).
8. Click **New** to create a new listener and ensure that the listener destination address is set to **Explicit** or to the **Destination Host** that is used for the OWA service and the action is set to **Intercept**. Click **OK** to dismiss the listener dialog. Click **OK** to dismiss the **Edit Service** dialog; click **Apply** in the Management Console. Click **OK** to dismiss the confirmation dialog.

### Configuring the Forwarding Host

The next task in this process is to define the location of the back-end server(s) to obtain the email content.

1. From the management console, go to **Configuration > Forwarding > Forwarding Hosts** as shown to the right.

2. Click on **New** to add a new forwarding host. Give the forwarding host an **Alias**, this example uses OWA, and enter the IP address of your OWA server as the **Host**. In this example, the OWA server is using HTTPS and is listening on port 443. In the case the OWA server is using HTTP, you have to modify the forwarding host settings accordingly.

Click **OK** to dismiss the Edit Service dialog; click **Apply** in the Management Console. Click **OK** to dismiss the confirmation dialog.
Configuring the Forwarding Policy

Next step is to add the forwarding rules to send requests to the OWA server.

1. From the management console, go to Configuration > Policy > Visual Policy Manager as shown below and click on Launch.

2. In VPM, begin by left-clicking Policy and selecting Add Forwarding Layer from the dropdown menu; this example names the layer Forwarding. Click OK to add the new layer.

3. Right-click the Destination setting and select Set. The Set Destination Object dialog displays.

4. Click New and select Server URL. The Add Server URL Object dialog displays.

   ![Add Server URL Object](image)

   Name: https_webmail.training.bluecoat.com
   
   Simple Match: URL:
   
   If the host specified is a domain name, all hosts in that domain (or any subdomain) will match. If a path is specified, all paths with that prefix will match. If a scheme or port number is specified, only URLs with that scheme or port will match.

   ![Advanced Match](image)

   Scheme: https
   Host: webmail.training.bluecoat.com
   Port: 80 or 1800-2000
   Path: Exact Match

   Click Add to add the Server URL object (wait until the dialog clears). Click Close to dismiss the dialog. The new destination object displays in the forwarding layer.

5. Click Advanced Match, select https as the Scheme, and enter the URL of your OWA as the Host. Name the object if you wish. Click Add to add the Server URL object (wait until the dialog clears). Click Close to dismiss the dialog. The new destination object displays in the forwarding layer.

6. Next, define forwarding of Web requests to your OWA server to the appropriate mail server: Right-click the Action setting and select Set. The Set Action Object dialog displays.

7. Click New and select Select Forwarding. The Add Select Forwarding Object dialog displays. Select your previously-defined forwarding host (OWA, in the example) and click Add to move it from the left-hand box to the right-hand box. Name the forwarding object if you wish; this example names the object “forwarding_OWA.” Click
OK to add the object and dismiss the dialog. The Set Action Object dialog re-displays. Click OK to set the object and dismiss the dialog.

8. The VPM displays the configured forwarding layer as shown below:

Click Install Policy to install the forwarding policy. Click OK to dismiss the confirmation dialog. Close the VPM window.

Note: requests to OWA have to be allowed in a Web Access Layer. This step is skipped here.

Configuring an external OWA URL on the Exchange Server

In the case the OWA server is using a different URL for external users than internal, you can configure this external URL on the Exchange Server. The advantage of doing this is, that there are no URL rewriting policies required on the reverse proxy.

On the Exchange Server, launch the "Exchange Management Console" and navigate to the Server Configuration > Client Access settings. Click on the Outlook Web App tab.

Right-click on owa (Default Web Site) and choose Properties. Here you can enter the external URL:
Configuring an external ActiveSync URL on the Exchange Server

In the case the ActiveSync server is using a different URL for external users than internal, you can configure this external URL on the Exchange Server. The advantage of doing this is, that there are no URL rewriting policies required on the reverse proxy.

On the Exchange Server, launch the “Exchange Management Console” and navigate to the Server Configuration > Client Access settings. Click on the Exchange ActiveSync tab.

Right-click on Microsoft-Server-ActiveSync (Default Web Site) and choose Properties. Here you can enter the external URL:

Configuring “HTTP to HTTPS” and “/” to “/owa” redirect Policies

To add re-directs for “webmail.training.bluecoat.com” or “http://webmail.training.bluecoat.com” to “https://webmail.training.bluecoat.com/owa” and for https://webmail.training.bluecoat.com/ to “https://webmail.training.bluecoat.com/owa”, follow these steps:

1. From the management console, go to Configuration > Policy > Visual Policy Manager as shown below and click on Launch

2. In the Visual Policy Manager, select the Web Access Layer that you are using to allow access to OWA and click Add Rule.

3. Click Move Rule to place the new rule above the existing one.
4. Right-click the **Destination** setting and select **Set**. The Set Destination Object dialog displays.

5. Click **New** and create a **Request URL** object with the following settings and add it as destination object to your policy:

![Request URL Object](image)

   Name: `webmail.training.bluecoat.com`
   
   - **Simple Match**
     - **URL:**
       
       If the host specified is a domain name, all hosts in that domain (or any subdomain) will match. If a path is specified, all paths with that prefix will match. If a scheme or port number is specified, only URLs with that scheme or port will match.

   - **Regular Expression Match**
     - **RegEx:**
   
   - **Advanced Match**
     - **Scheme:** `http`
     - **Host:** `webmail.training.bluecoat.com`
     - **Port:** `e.g. 80 or 1800-2000`
     - **Path:**

6. Next, right-click the **Action** setting and select **Set**. The Set Service Object dialog displays.

7. Click **New** and select **Combined Action**. The Add Combined Action object dialog displays.

   ![Combined Action Object](image)

   **Add Allow** to the **Selected Action Objects** list.

   Click **New** and create a **Return Redirect** action with the following settings and add it to the **Selected Action Objects** list, too:

   ![Return Redirect Object](image)

   **Name:** `redirect_owa`
   
   **Response code:** 301, 302, 307
   
   **URL:** `https://webmail.training.bluecoat.com`

   Click **OK** to set the object as action. This is how your policy should look like now:

![Combined Action Object](image)

8. Click **Install Policy** to finish.

9. One use case is still missing: redirect https://webmail.training.bluecoat.com requests to https://webmail.training.bluecoat.com/owa. Add a new rule below the just added rule by following the steps described in step “2”.

10. Right-click the **Destination** setting and select **Set**. The Set Destination Object dialog displays.
11. Click New and create a Request URL object with the following settings and add it as destination object to your policy:

- **Name**: https_webmail.training.bluecoat.com/
- **URL**: 
- **If the host specified is a domain name, all hosts in that domain (or any subdomain) will match. If a path is specified, all paths with that prefix will match. If a scheme or port number is specified, only URLs with that scheme or port will match.**

12. Next, right-click the Action setting and select Set. The Set Service Object dialog displays. Select the previously configured combined action object as action for this rule, too. Click OK to set the object as action.

In the case ActiveSync will be used over the same Reverse Proxy, request to the ActiveSync URLs should not be redirected to “/owa”. The URL for ActiveSync will be the one that has been configured on the ActiveSync server as “external URL”. In this example it is https://webmail.training.bluecoat.com/Microsoft-Server-ActiveSync. The following 3 steps describe how to configure this:

13. Click in Add Rule and move the new rule to the top.
14. Right-click the destination field and then left-click on Set > New and add a new Request URL object. Configure the ActiveSync URL as shown in the following screenshot and click on OK and OK to set this object as destination object:

15. Right-click on the action field and left-click on Allow.
16. This is how your policy should look like:

17. Click Install Policy to finish and close the VPM.
18. In order to accept HTTP requests on port 80, a HTTP service has to be created for OWA:

From the management console, go to Configuration > Services > Proxy Services. Select New Service and configure a service with the following settings:
Enter the IP address that is used for the external OWA URL in the IP Address field.

19. Click Apply to finish after you have added the new service.

Results:
Now, if your users enter “webmail.training.bluecoat.com” or “http://webmail.training.bluecoat.com” or “https://webmail.training.bluecoat.com” they are redirected to https://webmail.training.bluecoat.com/owa. ActiveSync requests will not be redirected.

Advanced Features
The following sections describe how to use and setup additional, advanced security features.

IWA (basic) or LDAP authentication with credential forwarding
By default, OWA is using forms based authentication:

To be able to achieve a single sign on user experience, and add an additional layer of security by requiring authentication at the reverse proxy, the following tasks have to be done:

1. Enable IWA (basic) or LDAP authentication. We are using IWA with forms based authentication (OWA) and origin authentication (ActiveSync) in this example.
2. Reconfigure OWA to require basic authentication instead of forms based authentication.

Enable IWA authentication at the reverse proxy
Note: detailed steps for adding an IWA realm are skipped here. For more information about IWA, please refer to the ProxySG documentation.

We are using an IWA-direct realm for this documentation. Kerberos and NTLM authentication options have been disabled. Credentials are secured by using HTTPS to access the authentication form on the ProxySG.

Reconfigure OWA to require basic authentication instead of forms based authentication
On the Exchange Server, launch the “Exchange Management Console” and navigate to the Server Configuration > Client Access settings. Click on the Outlook Web App tab.
Right-click on owa (Default Web Site) and chose Properties. Change to the Authentication tab. Change the authentication settings to Basic Authentication.

After this change you have to restart IIS. ActiveSync does not support authentication mechanisms other then basic, there are no changed required.

Single Sign On Policy (credential forwarding) on ProxySG - OWA
In order to secure the credential transport between client and ProxySG and in order to provide a user friendly landing page for OWA, we are using forms based authentication on ProxySG.

Follow these steps to add a new authentication form:

1. From the management console, go to Configuration > Authentication > Forms and click on New.
2. Configure a new authentication form object like this example:

I have slightly modified the text of the authentication form. The most important change is the addition of the following line: 

`<P>Please enter your email address as username!`

If users would just enter their username without domain information, credential forwarding and single sign on is not successful. However entering an email address to get access to OWA should not be unusual for an end user.

3. From the management console, go to Configuration > Policy > Visual Policy Manager as shown below and click on Launch


5. Add 2 new rules by clicking on Add Rule twice.

6. Right-click on the destination field in the first rule, then click on Set > New and add a new Request URL object with the following settings (for http://webmail.training.bluecoat.com):

The action should be set to None. This can be done by right-clicking the action field > Delete. The reason is, that HTTP requests should be redirected to HTTPS first. If the HTTP request would be authenticated first, the credentials would be sent in clear text from client to ProxySG. Another solution would be to use a redirect authentication mechanism; however, this is more complex then redirecting the request itself to https first. This policy will most probably be implemented anyway, because users have to use HTTPS to get access to OWA.
7. The second rule will be used to authenticate the users and to automatically forward credentials to OWA. Right-click on the Destination field in the second rule, then click on Set > New and add a new Request URL object with the following settings (for https://webmail.training.bluecoat.com):

8. Right-click on the action field in the second rule and click Set > New > Combined Action Object. Then click on New > Send Credentials Upstream and add an object with the following settings to the Selected Actions Objects list:

9. Then click on New > Authenticate and add an object with the following settings to the Selected Actions Objects list:

10. This is how your combined action object should look like:

11. Use the new combined action object as action for the second rule. Your policy should look like this now:

12. Click Install Policy to finish and close the VPM.
User Experience
After sending a request to https://webmail.training.bluecoat.com/owa, the user will see the following page:

Firefox on Mac:

Mobile Safari on iPhone:

Once the user has entered correct user credentials in the authentication form, ProxySG will authenticate the user at OWA transparently in the background and the user gets access to her/his OWA mailbox:

Firefox on Mac:

Mobile Safari on iPhone:

Single Sign On Policy (credential forwarding) on ProxySG – ActiveSync
The SSO configuration added for OWA can also be used for ActiveSync. ProxySG will be able to verify the user credentials and forward them to the ActiveSync server. In addition to the OWA related policy, a new authentication policy is required. ActiveSync does not support forms based authentication, it has to be basic authentication. The URL for ActiveSync will be the one that has been configured on the ActiveSync server as “external URL”. In this example it is https://webmail.training.bluecoat.com/Microsoft-Server-ActiveSync.

The following screenshots show an example of an Apple iOS configuration:

The following steps describe how to add the required policy for ActiveSync:

1. From the management console, go to Configuration > Policy > Visual Policy Manager as shown below and click on Launch
2. Go to the Web Authentication Layer and add a new rule by clicking on Add Rule. Move the new rule to the top.

3. Right-click on the destination field and select the ActiveSync URL object that has been created in the basic reverse proxy chapter (called active_sync in this example). Set this object as destination object.

4. Right-click on the action field click Set > New > Combined Action Object. Then click on New > Authenticate and add an object with the following settings to the Selected Actions Objects list:

5. Then add the existing Send Credentials Upstream, object that has been created for the OWA policy, to the Selected Actions Objects list:

6. This is how your combined action object should look like:

7. Use the new combined action object as action for this rule. Your policy should look like this now:

8. Click on Install Policy to finish and close the VPM.

**Kerberos Constrained Delegation for OWA**

**Why Kerberos Constrained Delegation (KCD)?**

Customers want to implement a Reverse Proxy where users are authenticated at the ProxySG. These users then need to be able to access authenticated content (for example their email) through the ProxySG. This means that the ProxySG needs to be able to securely send credentials to the OCS so that it knows what content to provide. Using KCD, the ProxySG is able to get a Kerberos ticket for the user from the Active Directory. This ticket can be used to securely authenticate the user at the OCS (OWA in this example).

KCD can only be used when the back end server does support integrated windows authentication, in particular Kerberos has to be supported. This is the case for OWA, but not for ActiveSync.

A note about the authentication mechanism between client and ProxySG: it basically does not matter what it is (forms-based, client certificates, etc.). Important is, that the user name used for authentication has the same syntax then the user name in the Active
Directory that is used for KCD. In the example below, a local realm has been used on the ProxySG to authenticate the user. The user name added to the local database was user01@training.bluecoat.com.

**Reconfigure OWA to require IWA authentication**

On the Exchange Server, launch the “Exchange Management Console” and navigate to the **Server Configuration > Client Access** settings. Click on the **Outlook Web App** tab.

Right-click on **owa (Default Web Site)** and chose **Properties**. Change to the **Authentication** tab. Change the authentication settings to **Integrated Windows Authentication**.

After this change you have to restart IIS.

**Verify that IIS supports the “Negotiate” authentication method**

Make sure that the “Negotiate” Authentication Provider is enabled for the OWA and ECP sites using the IIS Manager:

**Register SPN**

In a default configuration, the OWA web site (on IIS) is running under a local system account. That means that a SPN needs to be registered for the computer object of the OWA server. If the IIS configuration has been modified and the service is using another account, you have to use this account for the SPN registration.

In this example, OWA (and IIS) are running on a server called “tee-exchange”. The SPN “webmail.training.bluecoat.com”, which is the external URL for OWA, has been registered using the setspn.exe tool on the Exchange server:
The `setspn -L` option can be used to list all of the SPNs that have been registered for this computer. You can see that there are two SPNs, one for the external and one for the internal OWA URLs.

Configure Delegation for the ProxySG Computer Object

The ProxySG’s computer object needs permissions for delegation. Go to the Domain Controller and edit the ProxySG’s computer object, in this example it is the “SGVA” object.

Select the “Delegation” Tab and select “Trust this computer for delegation to specified services only” and add the previously specified SPN:

Note: You have to select “Use any authentication protocol”. “Use Kerberos only” would require clients to authenticate at the ProxySG using Kerberos. If you change this setting after you have tried KCD and it has failed, you have to reboot the ProxySG, otherwise it will continue to use a cached non-forwardable Kerberos ticket until it expires and this change will not have any effect.
Single Sign On Policy (KCD) on ProxySG

1. From the management console, go to Configuration > Policy > Visual Policy Manager as shown below and click on Launch.

![Configuration screenshot]

2. Add a Web Authentication Layer

3. Add a new rule by clicking on Add Rule.

4. The source field can be ignored, it has only been used for testing purposes.

5. Right-click on the action field. Then click on New > Authenticate and add the REALM that should be used to authenticate the client at the ProxySG.

6. Add a second Web Authentication Layer

7. Add a new rule by clicking on Add Rule.

8. Right-click on the action field. Then click on New > Kerberos Constrained Delegation and add the IWA REALM that should be used to authenticate the client at the OWA server. Authentication type has to be origin if the ProxySG is talking to the OWA server directly.

![Policy configuration screenshot]

Just for reference: here is the CPL of the above VPM-policy:

```
<Proxy>
client.address=192.168.178.222/32 authenticate(OWA_Local)
authenticate.force(no) authenticate.mode(auto)
<Proxy>
client.address=192.168.178.222/32 url.domain="webmail.training.bluecoat.com/owa" server.authenticate.constrained_delegation(origin,iwa)
```

User Experience

The OWA user gets prompted for authentication by the ProxySG. Once the user has been successfully authenticated, he gets access to OWA without any further authentication prompt.
Verify that the user has been authenticated using KCD

On the Exchange server, open the Windows event viewer and go to the Security logs. There you should be able to find a “logon” event after the user has connected to OWA and has been authenticated using KCD by the ProxySG. The event log should look like the following example:

![Event Logs Example](image)

Here you can see the user name, IP address of the ProxySG and a section called “Transited Services”. There you will see the ProxySG’s name (SGVA$@TRAINING.BLUECOAT.COM in this example).

Conclusion

The Blue Coat ProxySG provides an enterprise with greater security by front-ending access to an Outlook Web App email server. The ProxySG acts as the termination point for HTTPS, offloading that service from the OWA server, and then forwarding the email requests to the OWA server for response. In addition, ProxySG can be configured to authenticate the user and perform single sign on at the backend OWA server. This feature provides another level of security for users accessing email across public web services and helps companies gain greater control of how their users access information using corporate resources.

Blue Coat empowers enterprises to safely and securely choose the best applications, services, devices, data sources, and content the world has to offer, so they can create, communicate, collaborate, innovate, execute, compete and win in their markets. Blue Coat is the trusted by 86 percent of the FORTUNE Global 500.