How to Integrate CA SiteMinder with the Barracuda Web Application Firewall

https://campus.barracuda.com/doc/4259868/

Overview

CA/Netegrity SiteMinder provides an infrastructure for centralized and secure policy management of websites. It uniquely identifies users before they are authenticated as named users, and manages user privileges to ensure that they access only authorized applications or operations.

Support for SiteMinder has been deprecated. Also, SiteMinder feature will NOT be available from Version 9.1.

Components in SiteMinder Setup

The two significant components of SiteMinder are:

- **Web Agents** – Integrated with a standard web server or application server to enable SiteMinder to manage web applications using predefined security policies.
- **Policy Server** – Provides Policy management and AAA functions within the SiteMinder framework.

To integrate the Barracuda Web Application Firewall with CA/Netegrity SiteMinder, perform the following steps:

1. Configure the Netegrity SiteMinder Policy Server
2. Configure the Barracuda Web Application Firewall
3. Verify the Setup

Configure the Netegrity SiteMinder Policy Server

The images captured in the following steps are taken from the **Netegrity SiteMinder Policy Server Version 6.0 SP4**. The screens may vary depending on the version you are using.

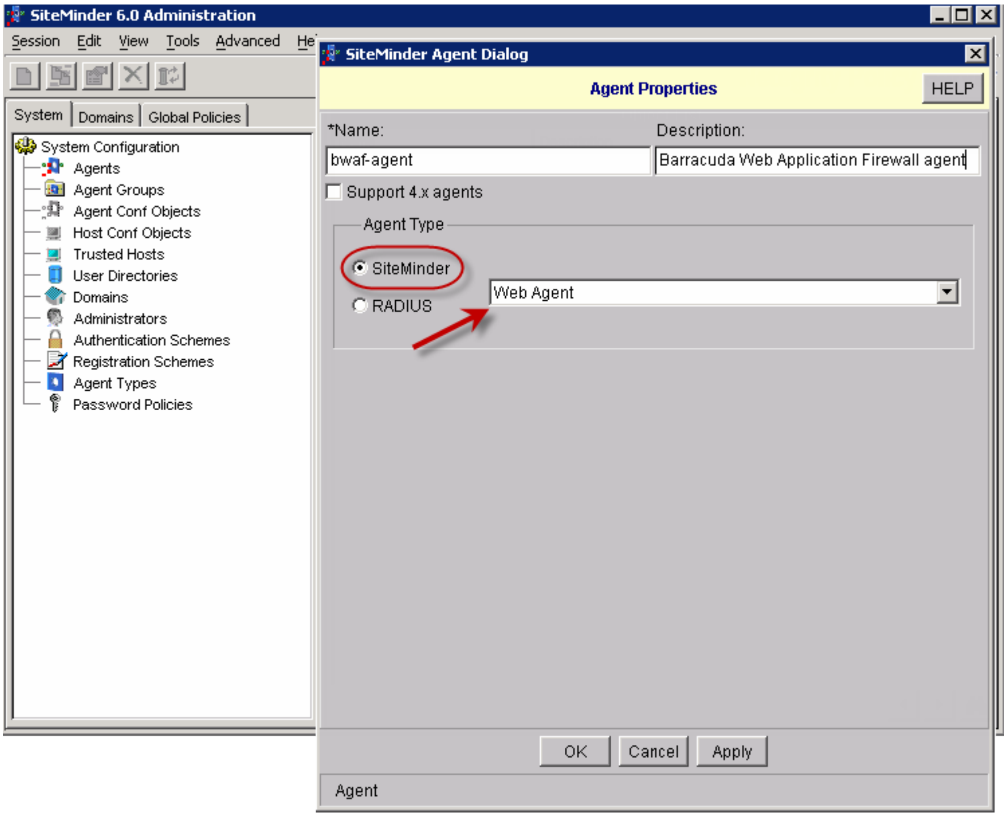
Follow these steps on the Netegrity SiteMinder Policy Server:

1. Create an Agent in the SiteMinder Policy Server
2. Create an Agent Configuration Object
3. Create a Host Conf Object
4. Create a User Directory with All User Names to be Authenticated by SiteMinder
5. Create a Domain for the User Directory
6. Create a Realm and Associate the Agent with the Realm
7. Create Rules for the Realm
8. Create a Policy for the Realm

Create an Agent in the SiteMinder Policy Server

1. From the **System** tab of the Netegrity Policy Server window, right click the **Agents** option from the **System Configuration** tree and select **Create Agent**. The Agent Properties window appears. To create the Agent, fill in the following fields:
    1. **Name** – Enter the agent name.
    2. **Description** – Enter the description for the agent.
    3. **Agent Type** – Select *SiteMinder* as agent type, and then select *Web Agent* from the drop-down list.
2. Click **Apply**, and then **OK**. The created agent appears in the Netegrity Policy Server window.

Figure 1. Creating SiteMinder Agent.



Agent Properties

*Name: bwaf-agent

Description: Barracuda Web Application Firewall agent

□ Support 4.x agents

Agent Type

● SiteMinder

○ RADIUS

Web Agent

Create an Agent Configuration Object

1. From the **System** tab of the Netegrity Policy Server window, right click the **Agent Conf Objects** option from the **System Configuration** tree. In the right hand pane, right click **ApacheDefaultSettings** and select **Duplicate Configuration Object** (Figure 2). The **Agent Configuration Object Properties** window appears. Fill in the following fields:
    1. **Name** – Enter a name for the agent configuration object.
    2. **Description** – Enter a description for the agent configuration object.
2. Click **Add**. The **Edit Parameter Dialog** appears. Provide the **Parameter Name**: *AcceptTPCookie* and **Value**: *Yes* and click **OK** (Figure 3).
3. Locate and select **DefaultAgentName** in the **Configuration Values**, and click **Edit**.
4. When the **Edit Parameter Dialog** appears, remove the hash (#) associated with the **DefaultAgentName** and enter the **Name** from step a. above in the **Value** field (Figure 4).
5. Verify the **RequireCookies** parameter in the **Configuration Values** is set to *Yes* for the agent.
6. Leave the remaining parameters set to their default values. Click **Apply** and then **OK**.

Figure 2. Agent Conf Object List.

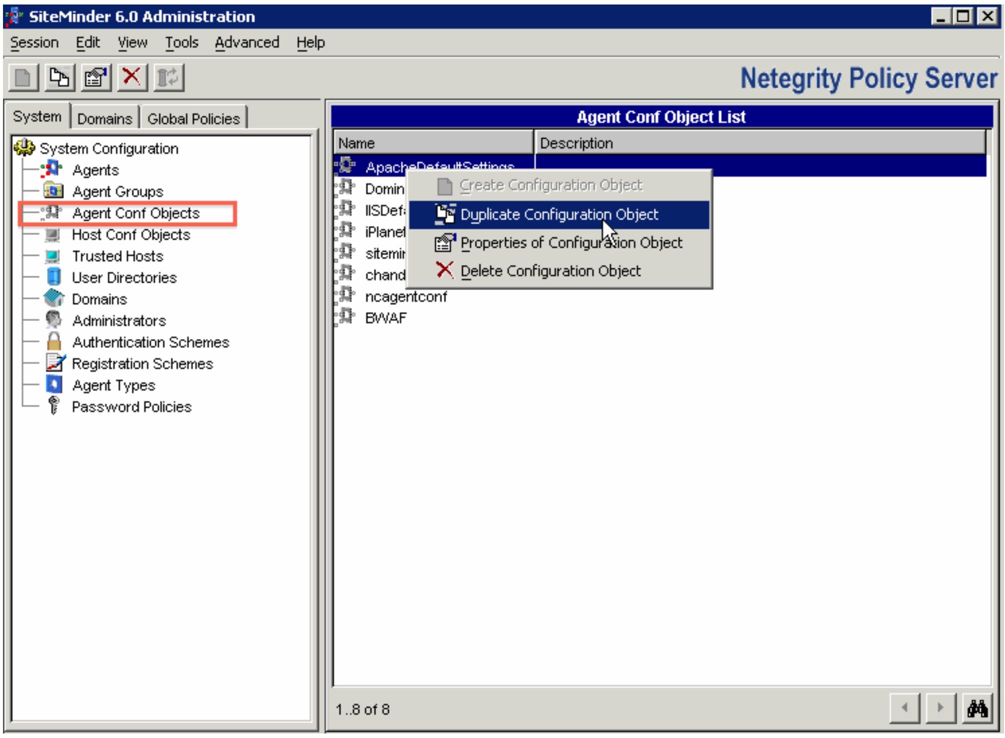
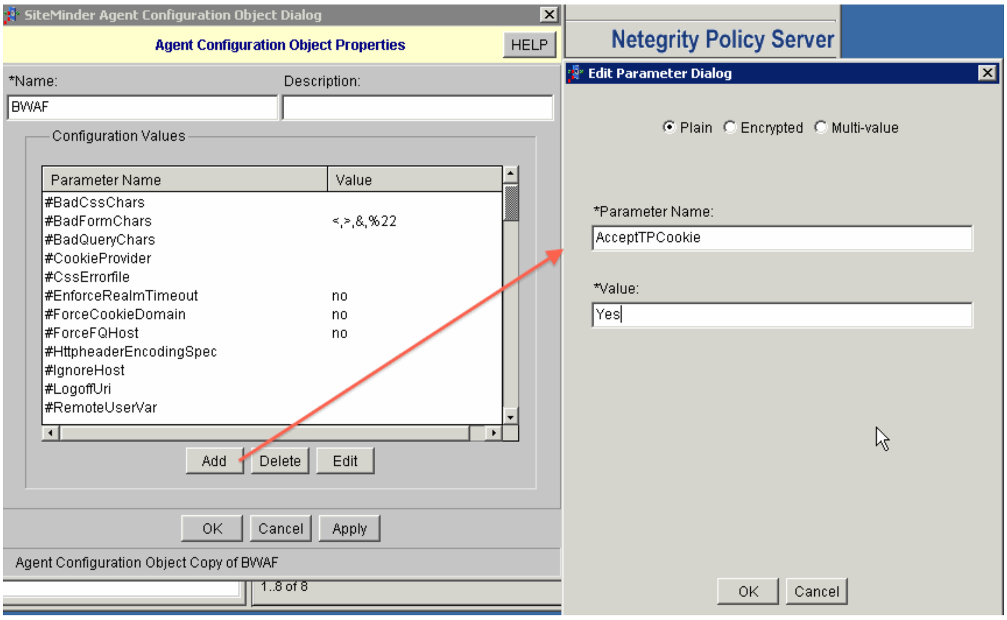


Figure 3. Agent Configuration Object Properties.



*Name: BWAF

Description:

Parameter Name	Value
#BadCssChars	
#BadFormChars	<,>,&,%22
#BadQueryChars	
#CookieProvider	
#CssErrorfile	
#EnforceRealmTimeout	no
#ForceCookieDomain	no
#ForceFQHost	no
#HttpheaderEncodingSpec	
#IgnoreHost	
#LogoffUri	
#RemoteUserVar	

Agent Configuration Object Copy of BWAF

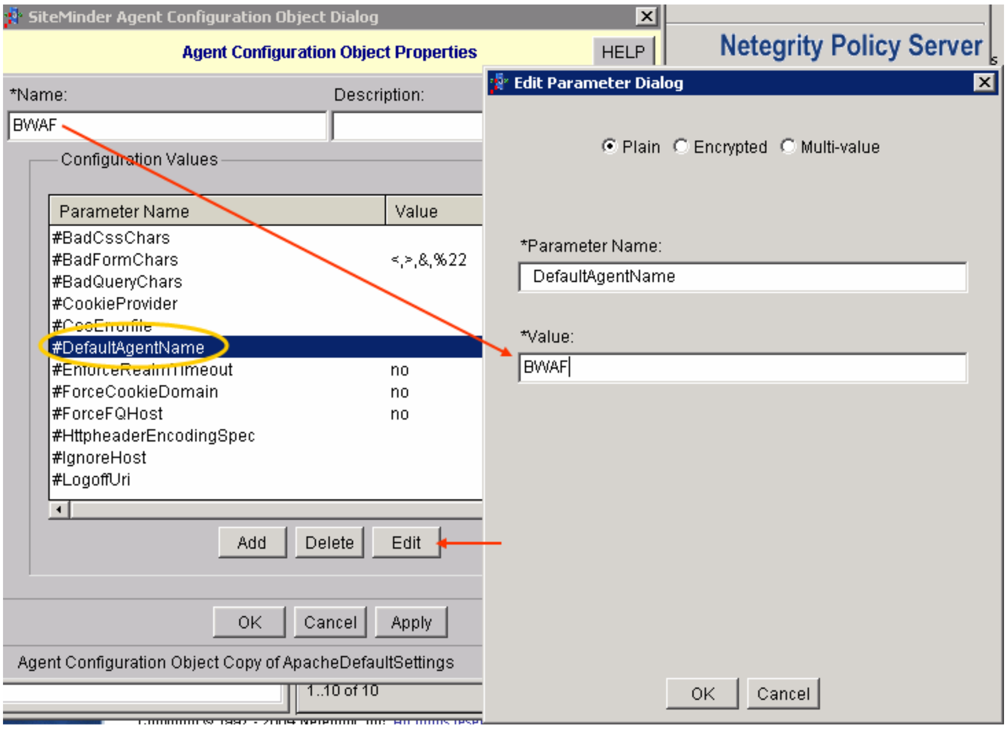
1..8 of 8

● Plain ○ Encrypted ○ Multi-value

*Parameter Name: AcceptTPCookie

*Value: Yes

Figure 4. Configuring Default Agent Name.



*Name: BWAF

Description:

Parameter Name	Value
#BadCssChars	
#BadFormChars	<,>,&,%22
#BadQueryChars	
#CookieProvider	
#CssErrorfile	
#DefaultAgentName	
#EnforceRealmTimeout	no
#ForceCookieDomain	no
#ForceFQHost	no
#HttpheaderEncodingSpec	
#IgnoreHost	
#LogoffUri	

Agent Configuration Object Copy of ApacheDefaultSettings

1..10 of 10

● Plain ○ Encrypted ○ Multi-value

*Parameter Name: DefaultAgentName

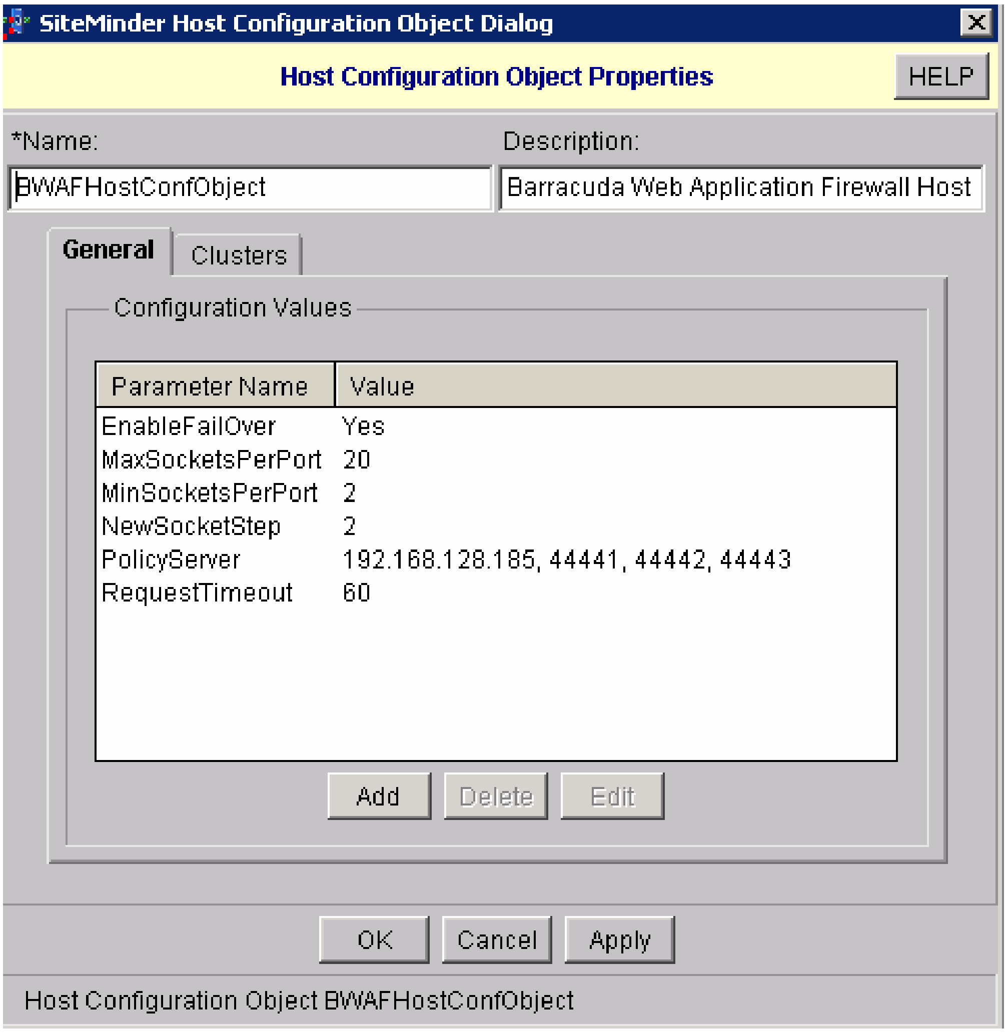
*Value: BWAF

Create a Host Conf Object

1. From the **System** tab of the Netegrity Policy Server window (Figure 1), right click the **Host Conf Objects** option from the **System Configuration** tree and click the **Create Host Conf Object**. The **Host Configuration Object Properties** window appears (Figure 5). Do the following to create the host configuration object:
   1. **Name**: Enter a name for the host configuration object.

2. **Description**: Enter a description for the host.
3. Click **Add**. The **Edit Parameter Dialog** window appears. Add the following parameters and set appropriate values. For example, see Figure 5.
    1. EnableFailOver
    2. MaxSocketsPerPort
    3. MinSocketsPerPort
    4. NewSocketStep
    5. PolicyServer
    6. RequestTimeout
2. Click **Apply** and then **OK**. The created Host Config Object appears in the Netegrity Policy Server window.

Figure 5. Host Configuration Object Properties.


SiteMinder Host Configuration Object Dialog
Host Configuration Object Properties
HELP
General
Clusters
Configuration Values
Add
Delete
Edit
OK
Cancel
Apply

*Name: BWAFHostConfObject

Description: Barracuda Web Application Firewall Host

Parameter Name	Value
EnableFailOver	Yes
MaxSocketsPerPort	20
MinSocketsPerPort	2
NewSocketStep	2
PolicyServer	192.168.128.185, 44441, 44442, 44443
RequestTimeout	60

Host Configuration Object BWAFHostConfObject

Create a User Directory with All User Names to be Authenticated by SiteMinder

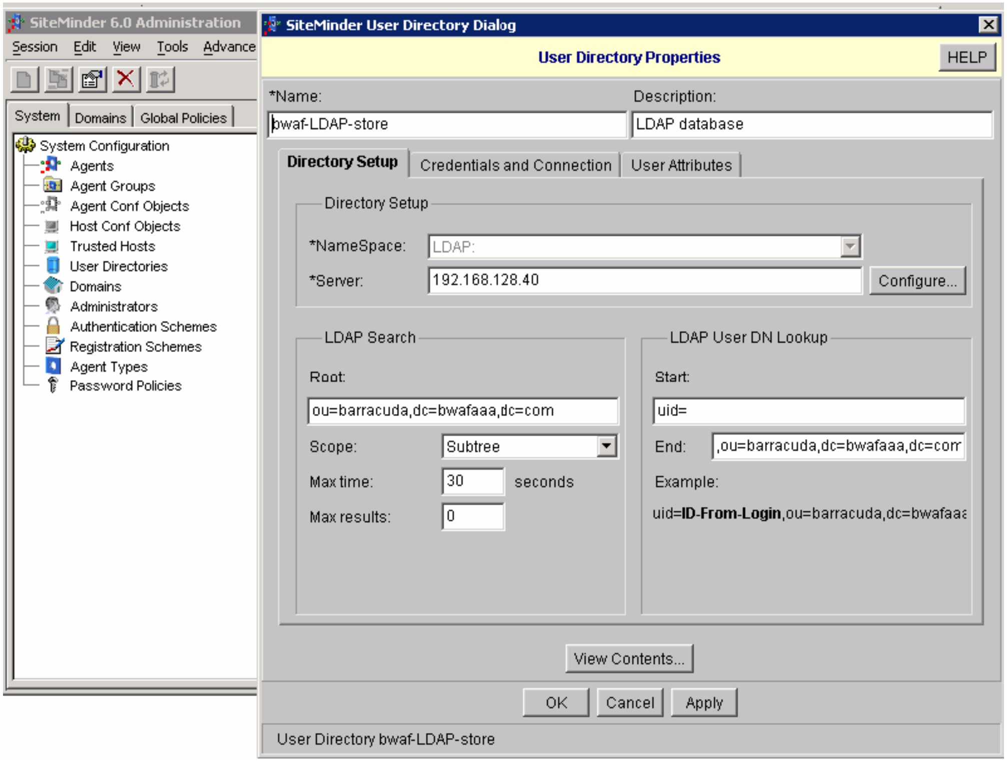
1. From the **System** tab of the Netegrity Policy Server window (Figure 1), right click the **User Directories** option from the **System Configuration** tree and click **Create User Directory**.

The **User Directory Properties** window (Figure 6) appears. Click the **Directory Setup** tab and do the following to configure the User Directory:

   1. **Name**: Enter a name for the user directory.
   2. **Description**: Enter a description.
   3. **NameSpace**: Select the directory where users can be authenticated.
   4. **Server**: Enter the IP Address of the **NameSpace** directory. SiteMinder communicates with this server to authenticate users.

2. Click the **Credentials and Connection** tab and configure the **Administrator Credentials** section:
   1. Select the **Require Credentials** check box.
   2. **Username**: Enter the Distinguished Name (DN) that can be used to query the LDAP server.
   3. **Password**: Enter the password for querying the LDAP server.
   4. **Confirm Password**: Reconfirm the password.
3. Click **Apply** and then **OK**. The created user directory appears in the Netegrity Policy Server window (Figure 7).

Figure 6. User Directory Properties.



*Name: bwaf-LDAP-store

Description: LDAP database

Directory Setup

*NameSpace: LDAP:

*Server: 192.168.128.40

LDAP Search

Root: ou=barracuda,dc=bwafaaa,dc=com

Scope: Subtree

Max time: 30 seconds

Max results: 0

LDAP User DN Lookup

Start: uid=

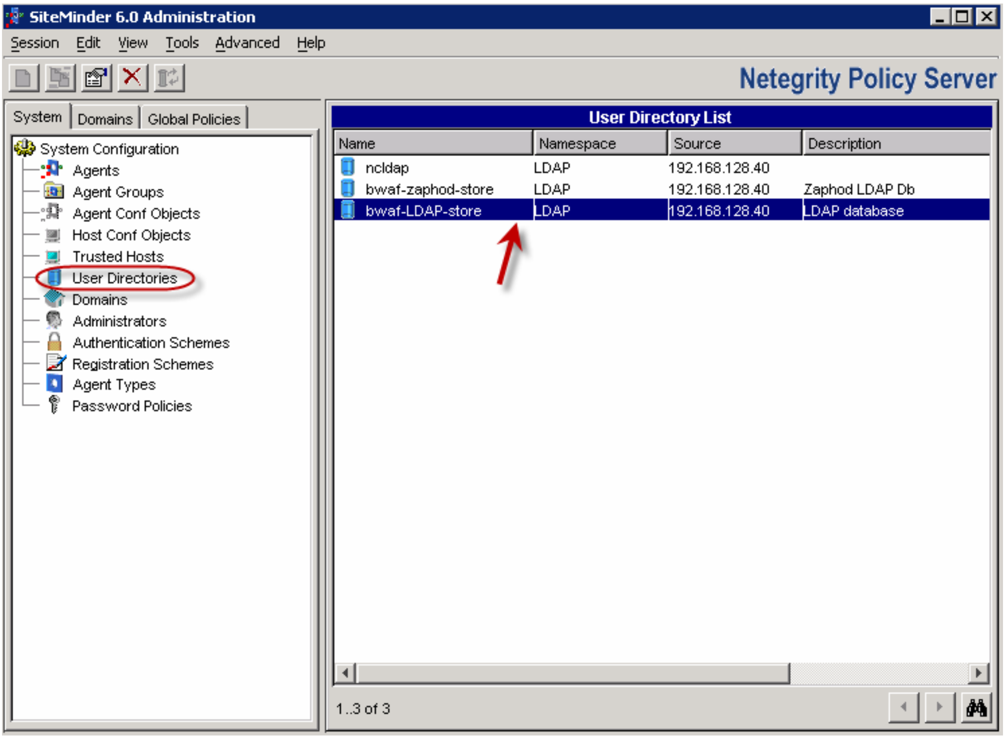
End: ,ou=barracuda,dc=bwafaaa,dc=com

Example:

uid=**ID-From-Login**,ou=barracuda,dc=bwafaaa

User Directory bwaf-LDAP-store

Figure 7. User Directory List.



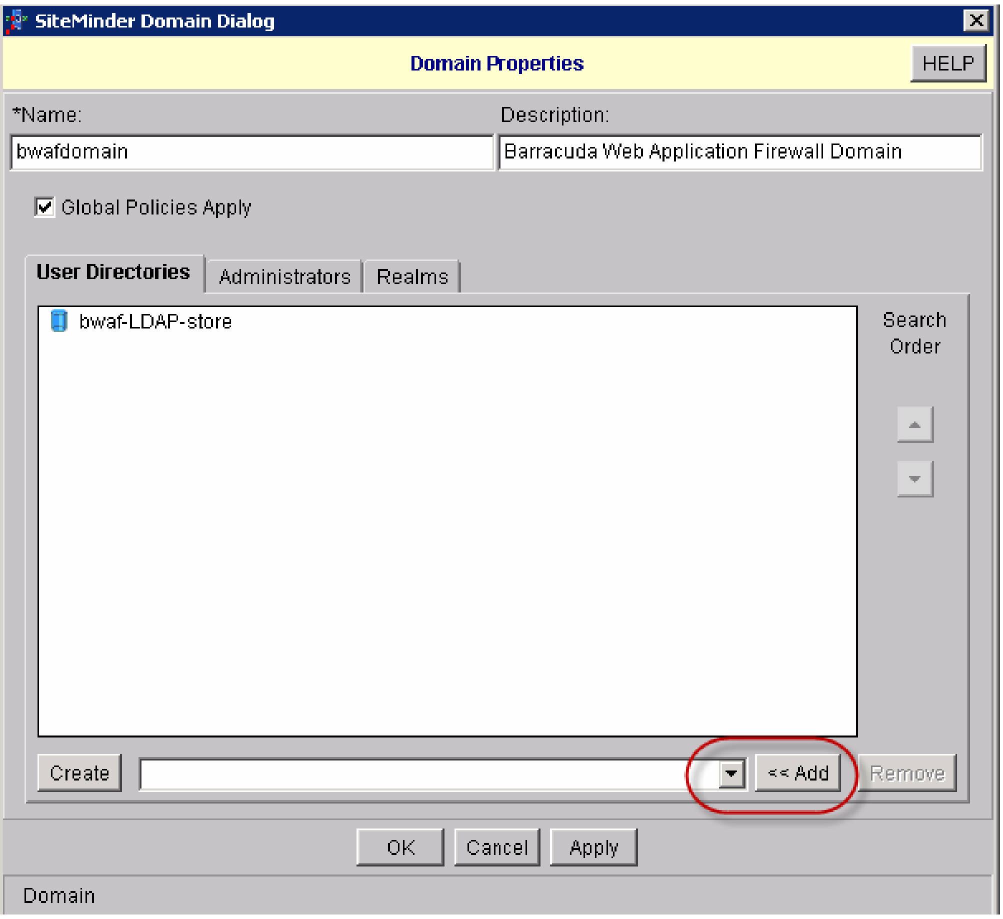
User Directory List

Name	Namespace	Source	Description
ncldap	LDAP	192.168.128.40	
bwaf-zaphod-store	LDAP	192.168.128.40	Zaphod LDAP Db
bwaf-LDAP-store	LDAP	192.168.128.40	LDAP database

Create a Domain for the User Directory

1. From the **System** tab of the Netegrity Policy Server window (Figure 1), right click the **Domains** option from the **System Configuration** tree and click **Create Domain**. When the **Domain Properties Dialog** (Figure 9) appears, do the following:
   1. **Name**: Enter a domain name.
   2. **Description**: Enter a description for the domain.
   3. In the **User Directories** tab, select the relevant directory and click **Add** (Figure 8).
2. Click **Apply** and then **OK**. The created agent appears in the Netegrity Policy Server window.

Figure 8. Domain Properties.



SiteMinder Domain Dialog

Domain Properties

*Name: bwafdomain

Description: Barracuda Web Application Firewall Domain

☑ Global Policies Apply

User Directories

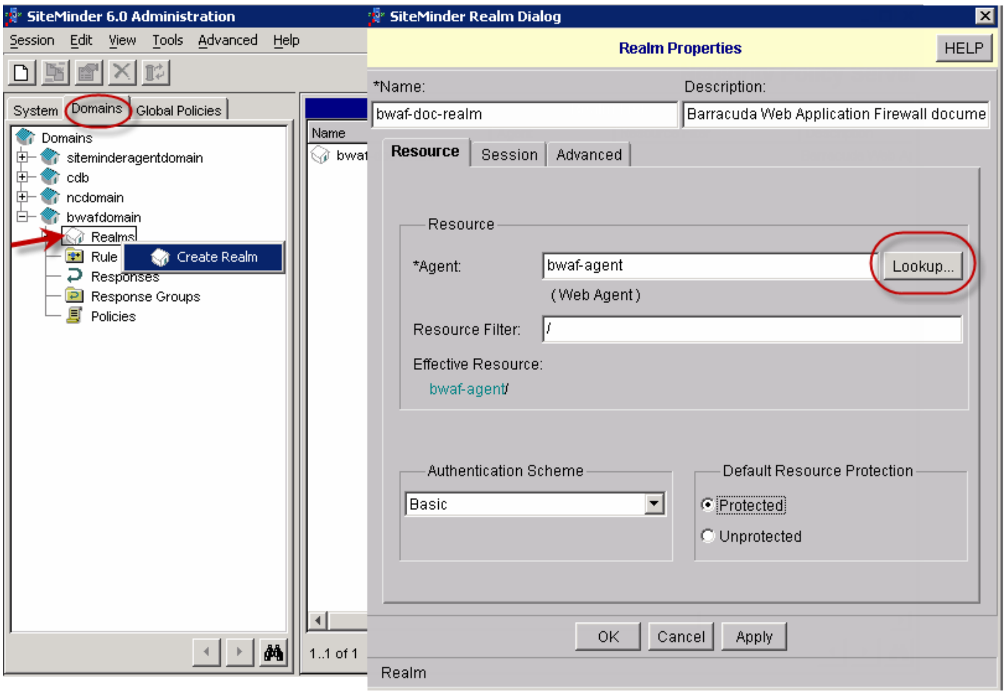
bwaf-LDAP-store

Create a Realm and Associate the Agent with the Realm

> Realm on the SiteMinder Policy Server is different from Realm on the Barracuda Web Application Firewall.

1. From the **Domains** tab of the Netegrity Policy Server window (Figure 9), right click the **Realm** option from the **Domains** tree and click **Create Realm**. When the **Realm Properties Dialog** (Figure 11) appears, do the following to create the realm:
    1. **Name**: Enter a realm name.
    2. **Description**: Enter a description for the realm.
2. Enter the name of the created agent in the **Agent** field, or click **Lookup** to select it from a list.
3. Select **Basic** or **HTML Form** authentication type from the **Authentication Scheme** list.
    1. If **Basic** authentication is selected, the Barracuda Web Application Firewall presents the default login page for authentication.
    2. If **HTML Form** authentication is selected, specify the target URL for authentication in the **Authentication Scheme Properties** window (Figure 10).
4. Click **OK** in the **Realm Properties** window to associate the agent with the created realm.

Figure 9. Domains.



*Name: bwaf-doc-realm

Description: Barracuda Web Application Firewall docume

Resource

*Agent: bwaf-agent

(Web Agent)

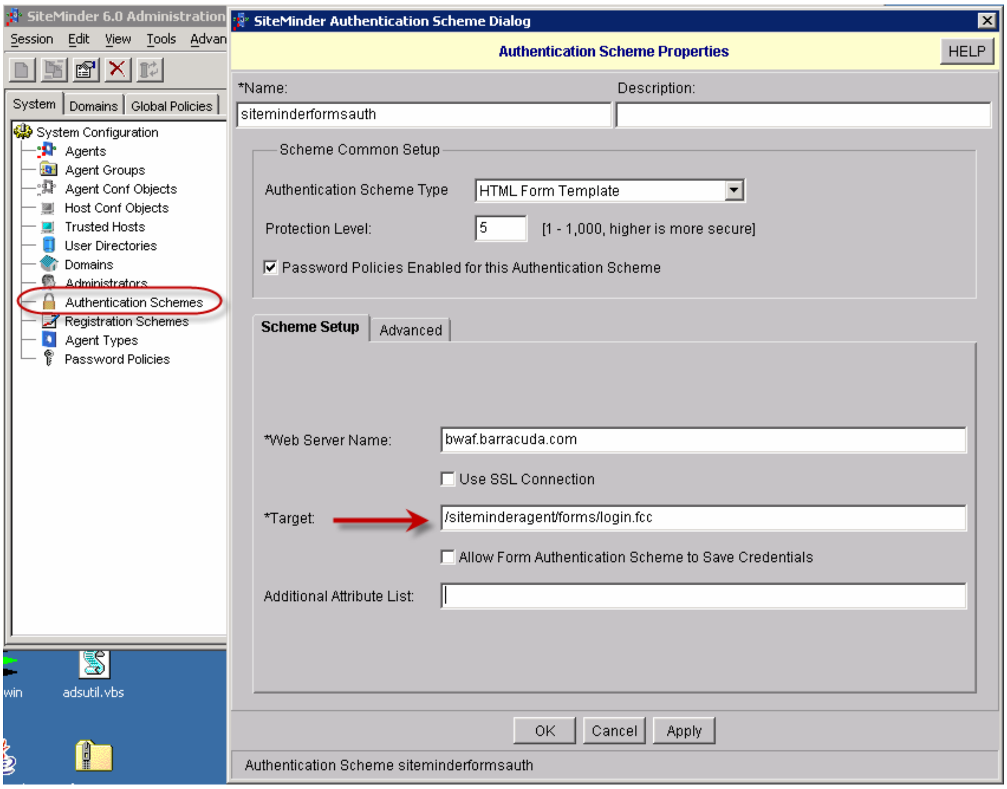
Resource Filter: /

Effective Resource: bwaf-agent/

Authentication Scheme: Basic

Default Resource Protection: ● Protected ○ Unprotected

Figure 10. Authentication Scheme.



*Name: siteminderformsauth

Description:

Scheme Common Setup

Authentication Scheme Type: HTML Form Template

Protection Level: 5 [1 - 1,000, higher is more secure]

☑ Password Policies Enabled for this Authentication Scheme

*Web Server Name: bwaf.barracuda.com

☐ Use SSL Connection

*Target: /siteminderagent/forms/login.fcc

☐ Allow Form Authentication Scheme to Save Credentials

Additional Attribute List:

Authentication Scheme siteminderformsauth

Create Rules for the Realm

Two rules needs to be configured for a realm:

- Rule for Authentication Event
- Rule for Web Agent actions

Rule for Authentication Event:

1. From the **Domains** tab of the Netegrity Policy Server window (Figure 9), click the **Realms** option from the **Domains** tree. Right click on the realm to which you want to add a rule and click **Create Rule under Realm** (Figure 11). When the **Rule Properties**window appears, do the following to configure the rule:
   1. **Name**: Enter a rule name.
   2. **Description**: Enter a description for the rule.
   3. Select **Authentication events** in the **Action** section (Figure 12).
2. Click **Apply** and then **OK**. The created rule appears in the list of rules and realms for the bwaf-doc-realm.

Figure 11. Creating a Rule.

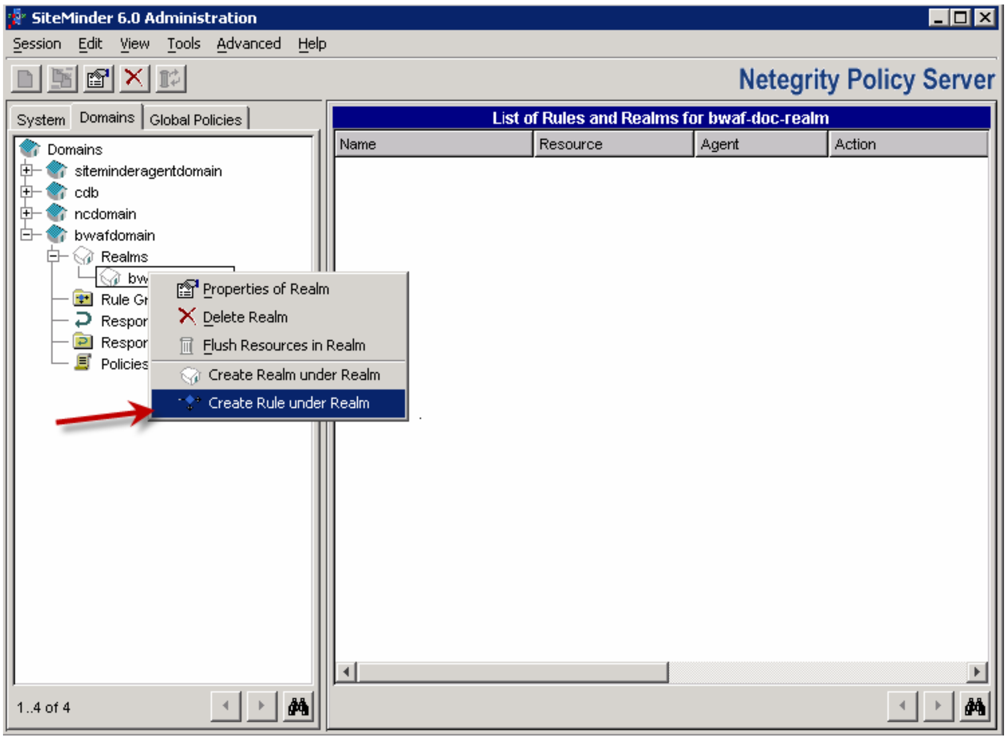
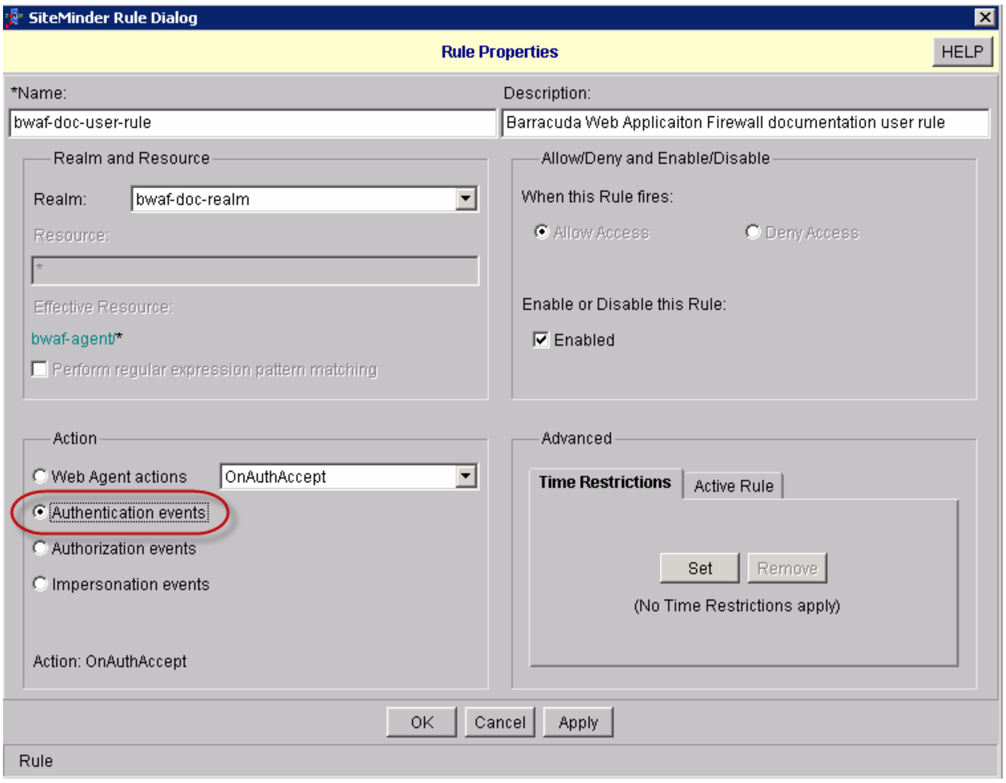


Figure 12. Rule Properties.



*Name: bwaf-doc-user-rule

Description: Barracuda Web Applicaiton Firewall documentation user rule

Realm and Resource

Realm: bwaf-doc-realm

Resource: *

Effective Resource: bwaf-agent/*

☐ Perform regular expression pattern matching

Allow/Deny and Enable/Disable

When this Rule fires: ● Allow Access ○ Deny Access

Enable or Disable this Rule: ☑ Enabled

Action

○ Web Agent actions OnAuthAccept

● Authentication events

○ Authorization events

○ Impersonation events

Action: OnAuthAccept

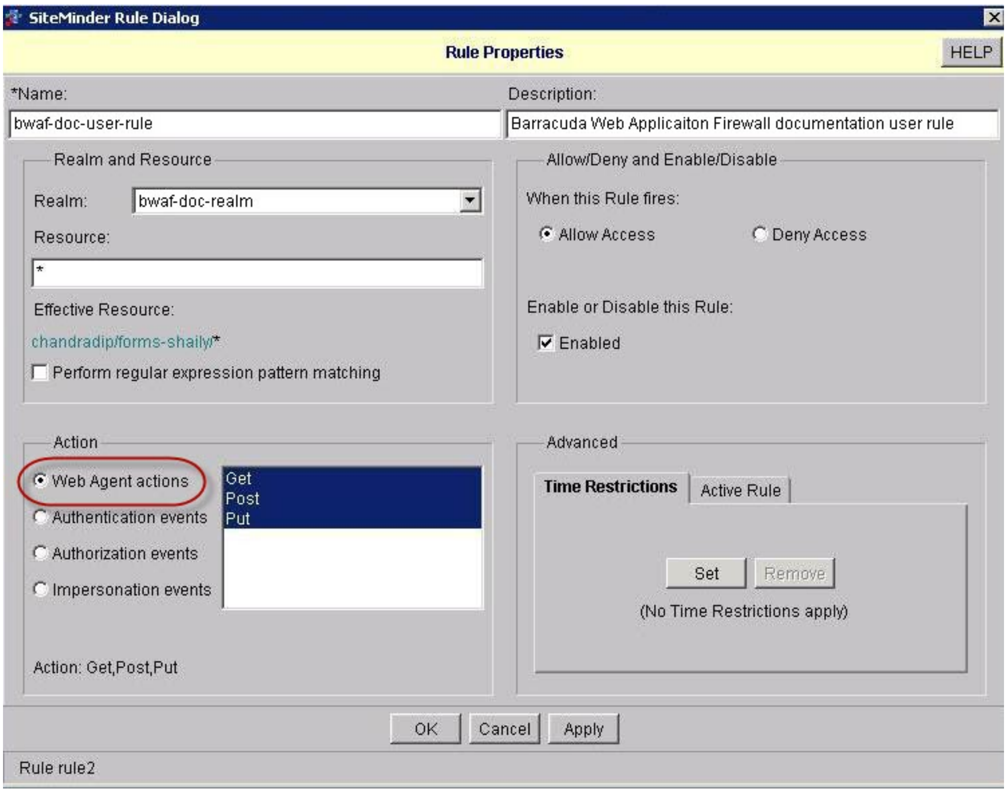
Advanced

(No Time Restrictions apply)

Rule for Web Agent Actions:

1. Follow **Step 1: a** and **b** under Rule for Authentication Event. In **Step 1: c**, select **Web Agent actions** in the **Action** section.
2. Select the methods for web agent (Figure 13). Click **Apply** and then **OK**.

Figure 13. Rule for Web Agent Actions.



SiteMinder Rule Dialog

Rule Properties

*Name: bwaf-doc-user-rule

Description: Barracuda Web Applicaiton Firewall documentation user rule

Realm and Resource

Realm: bwaf-doc-realm

Resource: *

Effective Resource: chandradip/forms-shaily/*

☐ Perform regular expression pattern matching

Allow/Deny and Enable/Disable

When this Rule fires:

● Allow Access ○ Deny Access

Enable or Disable this Rule:

☑ Enabled

Action

● Web Agent actions

○ Authentication events

○ Authorization events

○ Impersonation events

Get

Post

Put

Action: Get,Post,Put

Advanced

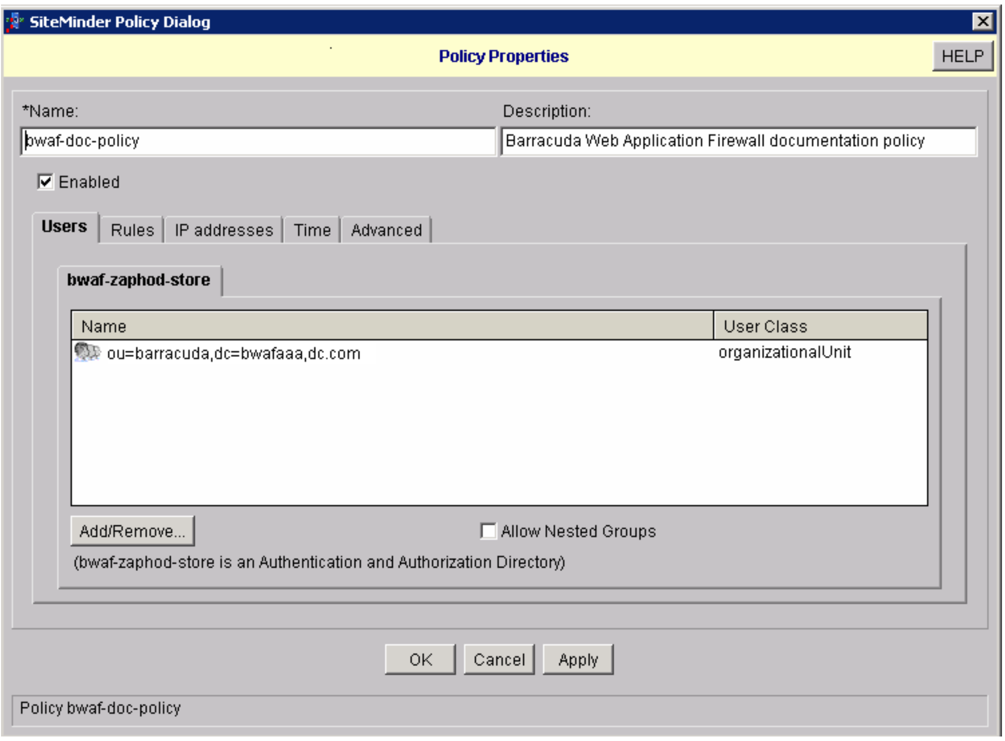
(No Time Restrictions apply)

Rule rule2

Create a Policy for the Realm

1. From the **Domain** tab of the Netegrity Policy Server window, click the **Policies** option from the **Domains** tree. Right click and select **Create Policy**. When the **Policies Properties** window appears , do the following to configure the policy:
2. In the **Users** tab, click the **Add/Remove** button. When the **Users/Groups** window appears, add the desired users and click **OK**. The added users appear in the Policy Properties window (Figure 14 - Users).
3. In the **Rules** tab, click the **Add/Remove Rules** button. When the **Rule Items** window appears, add the rules and click **OK**. The added rules appear in the **Policy Properties** window (Figure 15 - Rules).
4. Click **Apply** and then **OK**. The created policy appears in the **Policy List**.

Figure 14. Users.



*Name: bwaf-doc-policy

Description: Barracuda Web Application Firewall documentation policy

☑ Enabled

bwaf-zaphod-store

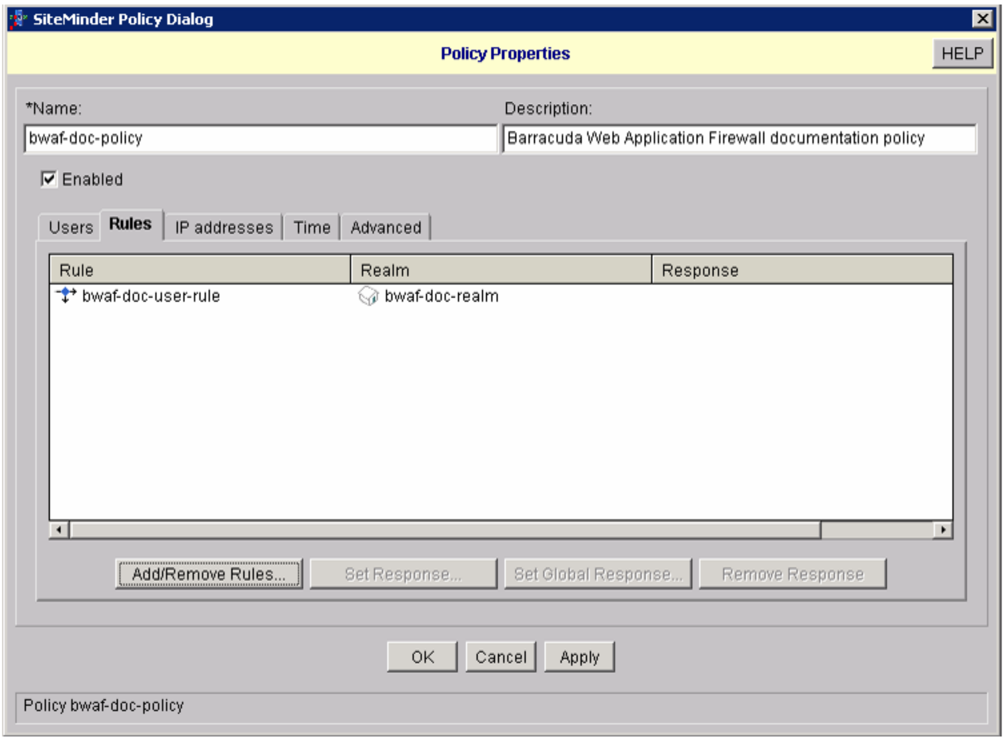
Name	User Class
ou=barracuda,dc=bwafaaa,dc.com	organizationalUnit

☐ Allow Nested Groups

(bwaf-zaphod-store is an Authentication and Authorization Directory)

Policy bwaf-doc-policy

Figure 15. Rules.



*Name: bwaf-doc-policy

Description: Barracuda Web Application Firewall documentation policy

☑ Enabled

Rule	Realm	Response
bwaf-doc-user-rule	bwaf-doc-realm	

Policy bwaf-doc-policy

The Barracuda Web Application Firewall can be integrated with an external CA web agent, which can act as a cookie provider application (master application) to the slave applications configured on the Barracuda Web Application Firewall.

Configure the Barracuda Web Application Firewall

Do the following steps to configure the Barracuda Web Application Firewall with CA SiteMinder:

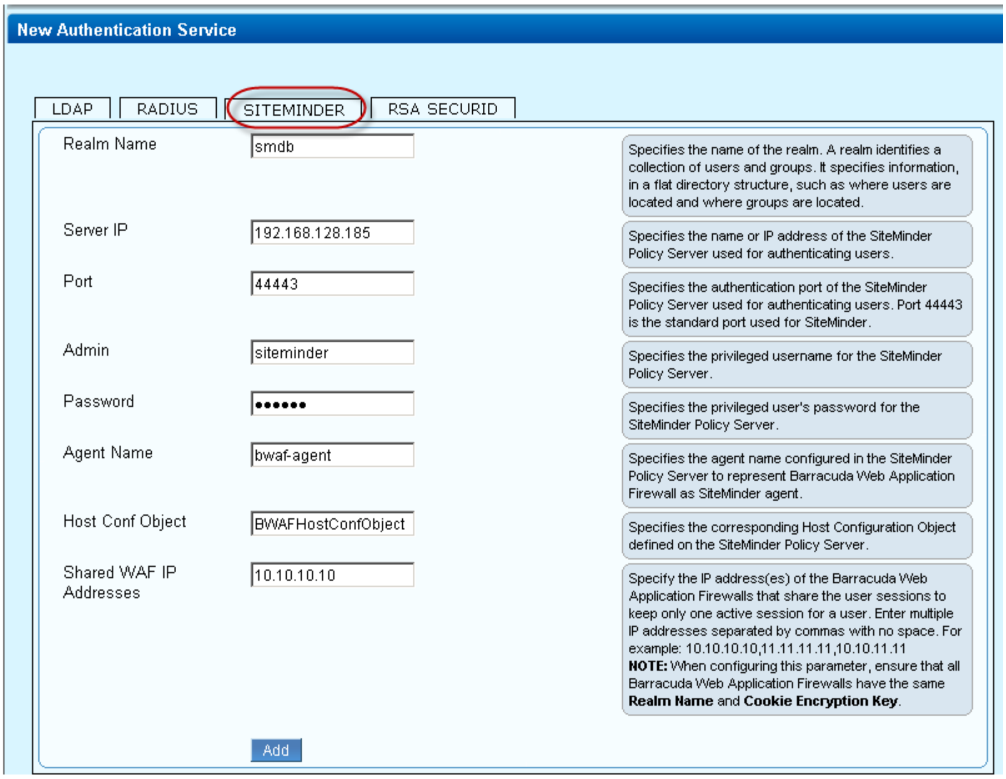
1. Add the SiteMinder Policy Server as an Authentication Service on the Barracuda Web Application Firewall
2. Bind the appropriate Service(s) with the SiteMinder Authentication Service
3. Configure the Authorization Policy for the Service

Add the SiteMinder Policy Server as an Authentication Service on the Barracuda Web Application Firewall

1. In the Barracuda Web Application Firewall web interface, go to the **ACCESS CONTROL > Authentication Services** page and select the **SITEMINDER** tab.
2. Specify values for the following fields:
   1. **Realm Name** – Enter the name of the realm where the Barracuda Web Application Firewall admins are stored.
   2. **Server IP** – Enter the IP address of the SiteMinder Policy Server used to authenticate users.
   3. **Port** – Enter the authentication port of the SiteMinder Policy Server. Port 44443 is the standard port used for SiteMinder.
   4. **Admin** – Enter the privileged username for the SiteMinder Policy Server.
   5. **Password** – Enter the privileged user password for the SiteMinder Policy Server.
   6. **Agent Name** – Enter the agent name configured in the SiteMinder Policy Server to act as the Barracuda Web Application Firewall's SiteMinder agent. Note: The specified agent name must have the following parameters set to *Yes* under **Agent Conf Objects** on the SiteMinder Policy Server:
      - AcceptTPCookie
      - RequireCookies
   7. **Host Conf Object** – Enter the corresponding Host Configuration Object defined on the SiteMinder Policy Server.
3. Click **Add** to add the SiteMinder server configuration.

When SiteMinder is initially accessed, a trusted host is generated on the SiteMinder Policy Server. It includes the Barracuda Web Application Firewall Serial Number and agent name.

Figure 16. SiteMinder Authentication Service Configuration.



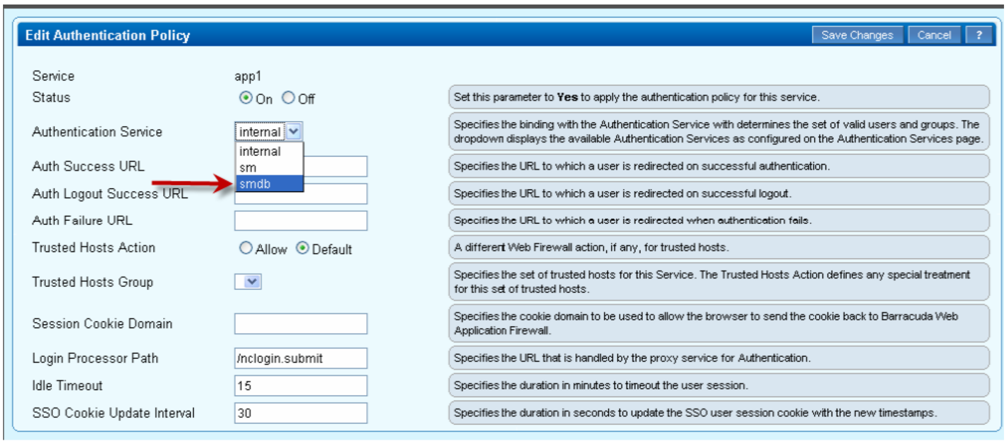
New Authentication Service

Realm Name	smdb	Specifies the name of the realm. A realm identifies a collection of users and groups. It specifies information, in a flat directory structure, such as where users are located and where groups are located.
Server IP	192.168.128.185	Specifies the name or IP address of the SiteMinder Policy Server used for authenticating users.
Port	44443	Specifies the authentication port of the SiteMinder Policy Server used for authenticating users. Port 44443 is the standard port used for SiteMinder.
Admin	siteminder	Specifies the privileged username for the SiteMinder Policy Server.
Password	••••••	Specifies the privileged user's password for the SiteMinder Policy Server.
Agent Name	bwaf-agent	Specifies the agent name configured in the SiteMinder Policy Server to represent Barracuda Web Application Firewall as SiteMinder agent.
Host Conf Object	BWAFHostConfObject	Specifies the corresponding Host Configuration Object defined on the SiteMinder Policy Server.
Shared WAF IP Addresses	10.10.10.10	Specify the IP address(es) of the Barracuda Web Application Firewalls that share the user sessions to keep only one active session for a user. Enter multiple IP addresses separated by commas with no space. For example: 10.10.10.10,11.11.11.11,10.10.11.11 **NOTE:** When configuring this parameter, ensure that all Barracuda Web Application Firewalls have the same **Realm Name** and **Cookie Encryption Key**.

Bind the appropriate Service(s) with the SiteMinder Authentication Service

1. Go to the **ACCESS CONTROL > Authentication** page.
2. Identify the Service you want to bind to the SiteMinder Authentication Service.
3. Click **Edit** next to the Service. When the **Edit Authentication Policy** window appears (Figure 17), do the following:
4. Set the **Status** to *On*.
5. Select the SiteMinder Authentication Service created above (Figure 16) from the list. Specify values for other parameter(s) and click **Save Changes**.

Figure 17. Authentication Policy.



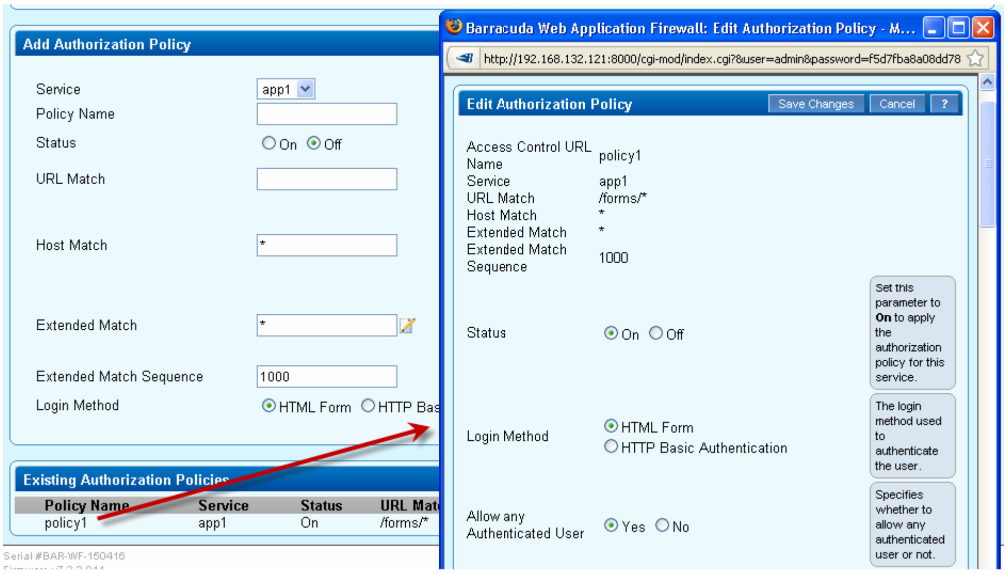
Edit Authentication Policy

Service	app1	
Status	● On ○ Off	Set this parameter to **Yes** to apply the authentication policy for this service.
Authentication Service	internal	Specifies the binding with the Authentication Service with determines the set of valid users and groups. The dropdown displays the available Authentication Services as configured on the Authentication Services page.
Auth Success URL		Specifies the URL to which a user is redirected on successful authentication.
Auth Logout Success URL		Specifies the URL to which a user is redirected on successful logout.
Auth Failure URL		Specifies the URL to which a user is redirected when authentication fails.
Trusted Hosts Action	○ Allow ● Default	A different Web Firewall action, if any, for trusted hosts.
Trusted Hosts Group		Specifies the set of trusted hosts for this Service. The Trusted Hosts Action defines any special treatment for this set of trusted hosts.
Session Cookie Domain		Specifies the cookie domain to be used to allow the browser to send the cookie back to Barracuda Web Application Firewall.
Login Processor Path	/nclogin.submit	Specifies the URL that is handled by the proxy service for Authentication.
Idle Timeout	15	Specifies the duration in minutes to timeout the user session.
SSO Cookie Update Interval	30	Specifies the duration in seconds to update the SSO user session cookie with the new timestamps.

Configuring Authorization Policy for the Service

1. Go to the **ACCESS CONTROL > Authorization > Add Authorization Policy** section.
2. **Service**: Select the desired service from the list.
3. **Policy Name**: Specify a name for the Authorization Policy.
4. Set the Status to *On* and specify the values for other parameter(s) as required.
5. Click **Add** to add the authorization policy configuration.
6. If you wish to enforce fine grained access control, click **Edit** next to the created policy. The **Edit Authorization Policy** window appears. For more detailed instructions, see Configuring Authorization Policy.

Figure 18. Authorization Policy.



Add Authorization Policy

Service	app1
Policy Name	
Status	○ On ● Off
URL Match	
Host Match	*
Extended Match	*
Extended Match Sequence	1000
Login Method	● HTML Form ○ HTTP Bas

Existing Authorization Policies

Policy Name	Service	Status	URL Mat
policy1	app1	On	/forms/*

Serial #BAR-WF-150416

Barracuda Web Application Firewall: Edit Authorization Policy - M...

http://192.168.132.121:8000/cgi-mod/index.cgi?&user=admin&password=f5d7fba8a08dd78

Edit Authorization Policy

Access Control URL Name	policy1	
Service	app1	
URL Match	/forms/*	
Host Match	*	
Extended Match	*	
Extended Match Sequence	1000	
Status	● On ○ Off	Set this parameter to **On** to apply the authorization policy for this service.
Login Method	● HTML Form ○ HTTP Basic Authentication	The login method used to authenticate the user.
Allow any Authenticated User	● Yes ○ No	Specifies whether to allow any authenticated user or not.

If the user realm is set to HTML Form authentication type on the SiteMinder Policy Server, the Login Method on the Barracuda Web Application Firewall must be set to HTML Form.

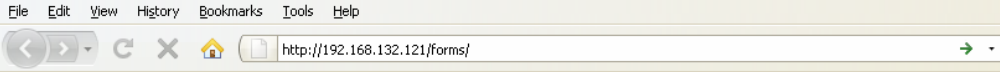
Verify the Setup

1. Enter the restricted URL in the browser. For example, for the above configuration you would enter http://192.168.132.121/forms/ in the address bar of a web browser (Figure 19).
2. If the user realm on the SiteMinder Policy Server is set to **Basic Authentication** type and the **Auth Not Done URL** field is blank on the **ACCESS CONTROL > Authorization** page, the Barracuda Web Application Firewall presents the default authentication page (Figure 20 -Default Authentication Page).
3. If the user realm on the SiteMinder Policy Server is set to **HTML Form** authentication type, the Barracuda Web Application Firewall redirects the user to the login URL specified in the

Authentication Scheme Properties window (Figure 10).

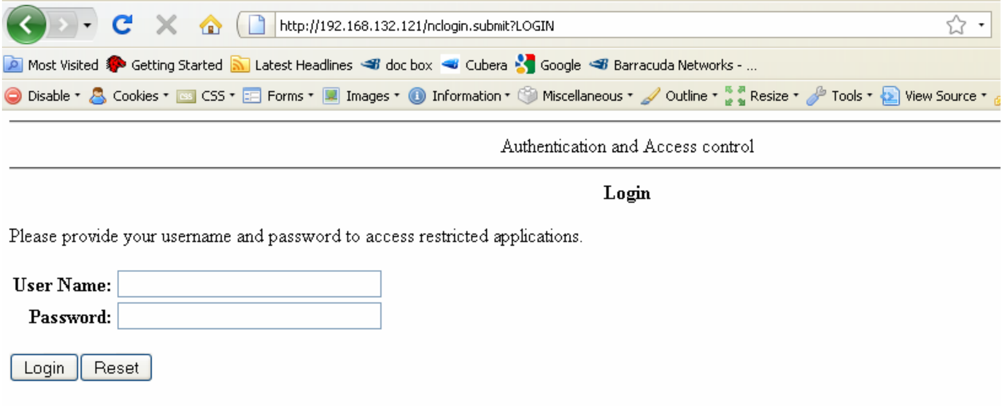
4. Go to the **BASIC > Access Logs** page (Figure 21), enable the login column and verify the results.

Figure 19. Address bar.



http://192.168.132.121/forms/

Figure 20. Default Authentication Page.



http://192.168.132.121/nclogin.submit?LOGIN

Authentication and Access control

Login

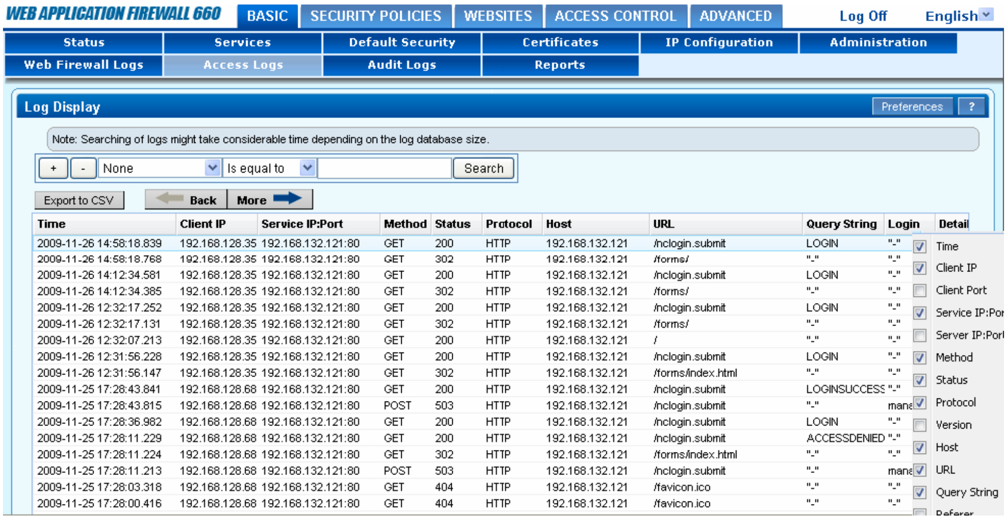
Please provide your username and password to access restricted applications.

User Name:

Password:

Login Reset

Figure 21. Access Logs.



Note: Searching of logs might take considerable time depending on the log database size.

None | Is equal to

Time	Client IP	Service IP:Port	Method	Status	Protocol	Host	URL	Query String	Login	Detail
2009-11-26 14:58:18.839	192.168.128.35	192.168.132.121:80	GET	200	HTTP	192.168.132.121	/nclogin.submit	LOGIN	"-"	
2009-11-26 14:58:18.768	192.168.128.35	192.168.132.121:80	GET	302	HTTP	192.168.132.121	/forms/	"-"	"-"	
2009-11-26 14:12:34.581	192.168.128.35	192.168.132.121:80	GET	200	HTTP	192.168.132.121	/nclogin.submit	LOGIN	"-"	
2009-11-26 14:12:34.385	192.168.128.35	192.168.132.121:80	GET	302	HTTP	192.168.132.121	/forms/	"-"	"-"	
2009-11-26 12:32:17.252	192.168.128.35	192.168.132.121:80	GET	200	HTTP	192.168.132.121	/nclogin.submit	LOGIN	"-"	
2009-11-26 12:32:17.131	192.168.128.35	192.168.132.121:80	GET	302	HTTP	192.168.132.121	/forms/	"-"	"-"	
2009-11-26 12:32:07.213	192.168.128.35	192.168.132.121:80	GET	200	HTTP	192.168.132.121	/	"-"	"-"	
2009-11-26 12:31:56.228	192.168.128.35	192.168.132.121:80	GET	200	HTTP	192.168.132.121	/nclogin.submit	LOGIN	"-"	
2009-11-26 12:31:56.147	192.168.128.35	192.168.132.121:80	GET	302	HTTP	192.168.132.121	/forms/index.html	"-"	"-"	
2009-11-25 17:28:43.841	192.168.128.68	192.168.132.121:80	GET	200	HTTP	192.168.132.121	/nclogin.submit	LOGINSUCCESS	"-"	
2009-11-25 17:28:43.815	192.168.128.68	192.168.132.121:80	POST	503	HTTP	192.168.132.121	/nclogin.submit	"-"	mana	
2009-11-25 17:28:36.982	192.168.128.68	192.168.132.121:80	GET	200	HTTP	192.168.132.121	/nclogin.submit	LOGIN	"-"	
2009-11-25 17:28:11.229	192.168.128.68	192.168.132.121:80	GET	200	HTTP	192.168.132.121	/nclogin.submit	ACCESSDENIED	"-"	
2009-11-25 17:28:11.224	192.168.128.68	192.168.132.121:80	GET	302	HTTP	192.168.132.121	/forms/index.html	"-"	"-"	
2009-11-25 17:28:11.213	192.168.128.68	192.168.132.121:80	POST	503	HTTP	192.168.132.121	/nclogin.submit	"-"	mana	
2009-11-25 17:28:03.318	192.168.128.68	192.168.132.121:80	GET	404	HTTP	192.168.132.121	/favicon.ico	"-"	"-"	
2009-11-25 17:28:00.416	192.168.128.68	192.168.132.121:80	GET	404	HTTP	192.168.132.121	/favicon.ico	"-"	"-"	

☑ Time
☑ Client IP
□ Client Port
☑ Service IP:Por
□ Server IP:Port
☑ Method
☑ Status
☑ Protocol
□ Version
☑ Host
☑ URL
☑ Query String
□ Referer

Figures