Application Note

Configuring Integrated Windows Authentication as a McAfee® Firewall Enterprise Authenticator

McAfee® Firewall Enterprise

version 7.x and 8.x

Use this Application Note to implement transparent browser authentication on McAfee® Firewall Enterprise version 7.x and 8.x. By working in conjunction with a Microsoft Windows® Domain Controller, users that are already logged into a domain can authenticate to the firewall transparently using NTLM.

You can also use this Application Note to configure McAfee SmartFilter® to use NTLM credentials.

In this document ...

Overview

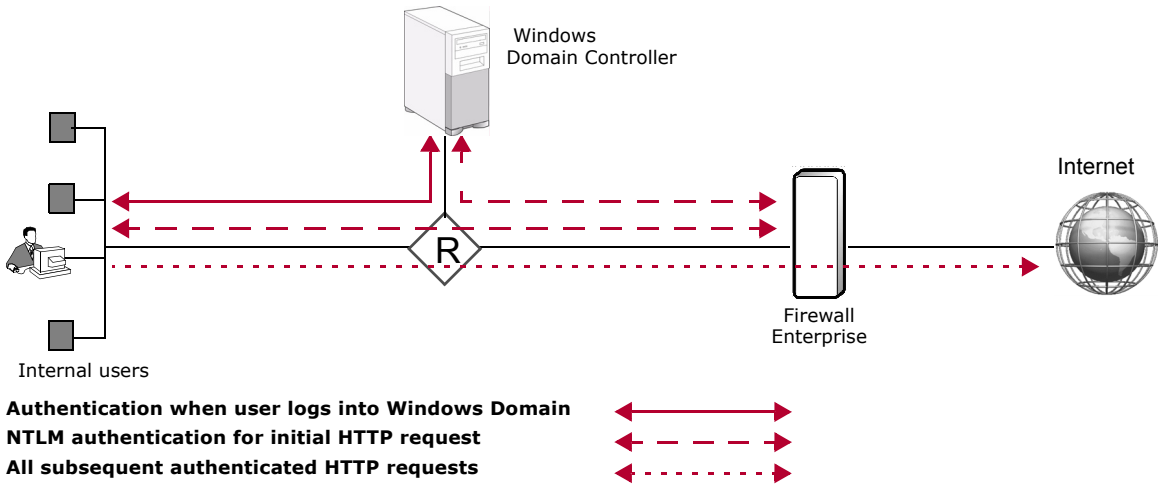
Configuring Integrated Windows Authentication (NTLM) as a McAfee® Firewall Enterprise authenticator allows users to authenticate HTTP or HTTPS connections without entering their credentials. By working in conjunction with a Windows Domain Controller (Windows DC), users who are already logged into a Windows domain can authenticate to the firewall transparently using NTLM.

You can also configure McAfee SmartFilter to apply Active Directory group-based policy by using NTLM credentials obtained by the firewall.

Refer to Figure 1. This diagram illustrates:

- The user is prompted for authentication when first logging into the Windows domain.
- The user does not receive additional prompts when connecting to the Internet.

Figure 1 Network diagram of Integrated Windows Authentication



Using Passport with NTLM

McAfee recommends using the Firewall Enterprise Passport authenticator in conjunction with NTLM. While NTLM authentication allows users to browse the web without being prompted for their credentials, there are authentication exchanges for each HTTP or HTTPS request. Each authentication exchange consists of multiple protocol messages for the client, Firewall Enterprise, and Windows DC. These exchanges can result in unnecessary load on the Windows DC, reduced performance, and unexpected authentication prompts for the client.

Use the Firewall Enterprise Passport authenticator in conjunction with NTLM to avoid these overhead-related issues. Since Passport caches the first successful NTLM authentication exchange, additional authentication exchanges on subsequent HTTP or HTTPS requests are not needed.

Configuration process

To set up Passport authentication with an NTLM authenticator, perform the following procedures:

1 *Configuring the Windows Domain Controller* on page 4

2 *Configuring the Firewall Enterprise* on page 8

3 *Configuring the users' browsers* on page 10

To configure McAfee SmartFilter to use NTLM credentials, see *Configuring McAfee SmartFilter and NTLM* on page 12.

Configuring the Windows Domain Controller

To configure your Windows DC to allow NTLM requests from Firewall Enterprise, perform the appropriate procedure:

- *Configuring Windows Server 2008* on page 4
- *Configuring Windows Server 2003* on page 6

Configuring Windows Server 2008

To configure a Windows Server 2008 DC, perform the following procedures:

1 *Modifying the Default Domain Controllers Policy* on page 4

2 *Modifying the Default Domain Policy* on page 5

3 *Making your configuration changes active* on page 6

Modifying the Default Domain Controllers Policy

To modify the Default Domain Controllers Policy:

1 Select **Start | Administrative Tools | Group Policy Management**. The Group Policy Management window appears.

2 In the Console Tree, expand **Forest: *your_domain* | Domains | *your_domain* | Group Policy Objects**, then right-click **Default Domain Controllers Policy** and select **Edit**. The Group Policy Management Editor appears.

3 In the Group Policy Management Editor Console Tree, expand **Computer Configuration | Policies | Windows Settings | Security Settings | Local Policies**, then select **Security Options**.

4 In the list of Policy items, right-click **Microsoft network server: Digitally sign communications (always)**, then select **Properties**. In the pop-up window that appears, perform the following steps:

   a Confirm that **Define this policy setting** is selected.

   b Select **Disabled**.

   c Click **OK**. The pop-up window closes.

5 In the list of Policy items, right-click **Network security: LAN Manager authentication level**, then select **Properties**. In the pop-up window that appears, perform the following steps:

   a Confirm that **Define this policy setting** is selected.

   b From the drop-down list, select one of the following options as appropriate for your network:

   - Send LM & NTLM responses
   - Send LM & NTLM – use NTLMv2 session security if negotiated
   - Send NTLM response only

   Note: Record your selection. You will use this setting in *Modifying the Default Domain Policy*.

   c Click **OK**. The pop-up window closes.

6 Close the Group Policy Management Editor. You return to the Group Policy Management window.

Modifying the Default Domain Policy

To modify the Default Domain Policy:

1 In the Group Policy Management window Console Tree, expand **Forest: *your_domain* | Domains | *your_domain***, then right click **Default Domain Policy** and select **Edit**. The Group Policy Management Editor appears.

2 In the Group Policy Management Editor Console Tree, expand **Computer Configuration | Policies | Windows Settings | Security Settings | Local Policies**, then select **Security Options**.

3 In the list of Policy items, right-click **Microsoft network server: Digitally sign communications (always)**, then select **Properties**. In the pop-up window that appears, perform the following steps:

   a Confirm that **Define this policy setting** is selected.

   b Select **Disabled**.

   c Click **OK**. The pop-up window closes.

4 In the list of Policy items, right-click **Microsoft network server: Digitally sign communications (if client agrees)**, then select **Properties**. In the pop-up window that appears, perform the following steps:

   a Confirm that **Define this policy setting** is selected.

   b Select **Disabled**.

   c Click **OK**. The pop-up window closes.

5 In the list of Policy items, right-click **Network security: LAN Manager authentication level**, then select **Properties**. In the pop-up window that appears, perform the following steps:

   a Confirm that **Define this policy setting** is selected.

   b From the drop-down list, select the option that you chose in *Modifying the Default Domain Controllers Policy*, Step 5.

   c Click **OK**. The pop-up window closes.

6 Close the Group Policy Management Editor and the Group Policy Management window.

Making your configuration changes active

By default, the Windows DC adopts the new policy within five minutes, and domain members adopt the new policy within two hours. To make your configuration changes effective immediately, perform the following steps.

1. Select **Start | Programs | Accessories | Command Prompt**. The Command Prompt window appears.
2. In the Command Prompt window, type **`gpupdate`**, then press **Enter**. When the command is complete, the following text appears:

```
User Policy update has completed successfully.

Computer Policy update has completed successfully.
```

The Windows DC is now configured to accept NTLM authentication requests from Firewall Enterprise.

Configuring Windows Server 2003

To configure a Windows Server 2003 DC, perform the following procedures:

1. *Modifying the Domain Controller Security Policy* on page 6
2. *Modifying the Domain Security Policy* on page 7
3. *Making your configuration changes active* on page 7

Modifying the Domain Controller Security Policy

To modify the Default Domain Controller Security Policy:

1. Select **Start | Administrative Tools | Domain Controller Security Policy**. The Default Domain Controller Security Settings window appears.
2. In the Console Tree, expand **Local Policies**, then select **Security Options**.
3. In the list of Policy items, right-click **Microsoft network server: Digitally sign communications (always)**, then select **Properties**. In the pop-up window that appears, perform the following steps:
   a. Confirm that **Define this policy setting** is selected.
   b. Select **Disabled**.
   c. Click **OK**. The pop-up window closes.
4. In the list of Policy items, right-click **Network security: LAN Manager authentication level**, then select **Properties**. In the pop-up window that appears, perform the following steps:
   a. Confirm that **Define this policy setting** is selected.
   b. From the drop-down list, select one of the following options as appropriate for your network:
      - Send LM & NTLM responses
      - Send LM & NTLM – use NTLMv2 session security if negotiated
      - Send NTLM response only

      Note: Record your selection. You will use this setting in *Modifying the Domain Security Policy* on page 7.
   c. Click **OK**. The pop-up window closes.
5. Close the Default Domain Controller Security Settings window.

Modifying the Domain Security Policy

To modify the Default Domain Security Policy:

1. Select **Start | Administrative Tools | Domain Security Policy**. The Default Domain Security Settings window appears.
2. In the Console Tree, expand **Local Policies**, then select **Security Options**.
3. In the list of Policy items, right-click **Microsoft network server: Digitally sign communications (always)**, then select **Properties**. In the pop-up window that appears, perform the following steps:
   a. Confirm that **Define this policy setting** is selected.
   b. Select **Disabled**.
   c. Click **OK**. The pop-up window closes.
4. In the list of Policy items, right-click **Microsoft network server: Digitally sign communications (if client agrees)**, then select **Properties**. In the pop-up window that appears, perform the following steps:
   a. Confirm that **Define this policy setting** is selected.
   b. Select **Disabled**.
   c. Click **OK**. The pop-up window closes.
5. In the list of Policy items, right-click **Network security: LAN Manager authentication level**, then select **Properties**. In the pop-up window that appears, perform the following steps:
   a. Confirm that **Define this policy setting** is selected.
   b. From the drop-down list, select the option that you chose in Step 4 on page 6.
   c. Click **OK**. The pop-up window closes.
6. Close the Default Domain Security Settings window.

Making your configuration changes active

By default, the Windows DC adopts the new policy within five minutes, and domain members adopt the new policy within two hours. To make your configuration changes effective immediately, perform the following steps.

1. Select **Start | Programs | Accessories | Command Prompt**. The Command Prompt window appears.
2. In the Command Prompt window, type **`gpupdate`**, then press **Enter**. When the command is complete, the following text appears:

```
User Policy Refresh has completed.

Computer Policy Refresh has completed.
```

The Windows DC is now configured to accept NTLM authentication requests from Firewall Enterprise.

Configuring the Firewall Enterprise

To use NTLM authentication, you must configure the Firewall Enterprise NTLM authenticator, Passport authenticator, and the HTTP rule(s) that will use the Passport authenticator.

Configuring authenticators

Two Firewall Enterprise authenticators must be used together to achieve transparent browser authentication with NTLM and Passport. You must first configure the NTLM authenticator so that the firewall can communicate with your Windows DC. Then, configure the Passport authenticator to cache credentials that are obtained by the NTLM authenticator.

Configuring an NTLM authenticator

The NTLM authenticator only needs to be set up once.

Note: If you have already configured an NTLM authenticator, no changes are needed.

To configure an NTLM authenticator:

1. Gather the IP address, port, and name of the target Windows Domain Controller you plan to use.
2. In the Admin Console, select **Policy | Rule Elements | Authenticators**.
3. Click the **New** icon and select **Windows**. The New Authenticator window appears.
4. Click **New** to add your Windows Domain Controller. Use the information gathered in Step 1 and click **Add.**

   Note: Ensure that the **Windows Domain Controller Name** is the system name of the controller and not the domain name.
5. In the Authentication method area, select **Transparent (NTLM)** and click **Add.**

   Note: The transparent authentication feature is supported with Windows Domain Controllers only. Other types of authentication servers are not supported.
6. Save your changes.

Configuring the Passport authenticator

Passport (previously known as Single Sign-On) works in conjunction with a specified authentication method to cache a user's initial authentication, thereby reducing authentication overhead and allowing access to multiple services with a single successful authentication to the firewall.

Configuring Passport for a version 7.x firewall

Perform these steps to configure Passport to cache NTLM credentials.

1. In the Admin Console, select **Policy | Rule Elements | Authenticators**.
2. Select **Passport** from the list of authenticators.
3. In the **Authenticators to establish Passport credentials** list, select the NTLM authenticator that you created in the *Configuring an NTLM authenticator* section.
4. From the **Default authenticator** drop-down list, select the NTLM authenticator that you created in the *Configuring an NTLM authenticator* section.
5. In the **Authenticators to establish Passport credentials** list, clear all other authenticators.
6. Make sure that **Require Web login** is deselected, then save your changes.

7 Verify that the Passport rule is enabled.

Note: The Passport rule must be enabled for Passport authentication to function.

a Select **Policy | Rules.** The Rules window appears.

b Select the rule titled **Passport.**

c If the Passport rule is disabled, click **Enable** in the toolbar.

d Save your changes.

Configuring Passport for a version 8.x firewall

Perform these steps to configure Passport to cache NTLM credentials.

1 In the Admin Console, select **Policy | Rule Elements | Passport**.

2 Click the **General** tab.

3 In the Establish passport credentials area, select the **Active** checkbox.

4 Under Authentication mode, select **Inband.**

5 In the **Authenticators to establish Passport credentials** list, select the NTLM authenticator that you created in the *Configuring an NTLM authenticator* section.

6 From the **Default authenticator** drop-down list, select the NTLM authenticator that you created in the *Configuring an NTLM authenticator* section.

7 In the **Authenticators to establish Passport credentials** list, clear all other authenticators.

8 Save your changes.

Adding NTLM authentication to rules

NTLM authentication is enforced via proxy rules on a per-rule basis. The following procedure explains how to enable NTLM authentication on HTTP traffic in conjunction with the Passport authenticator.

Enabling NTLM authentication for a version 7.x firewall

Perform these steps to enable NTLM authentication for HTTP traffic.

1 Select **Policy | Rules.**

- If you are creating a new rule, click **New Rule,** then fill in the Name, Source, and Destination areas.
- If you are modifying an existing rule, select the rule, then click **Modify**.

2 In the **Service** field, select or verify the HTTP proxy service the rule will use.

If you want to allow HTTPS connections as well, create a service group that contains both HTTP and HTTPS proxies, and select that service group on the rule.

Note: McAfee recommends the non-transparent HTTP (NT-HTTP) connection type. If your rule allows transparent HTTP and HTTPS connections, users must visit a non-encrypted site (HTTP) before visiting encrypted sites (HTTPS).

3 From the **Authenticator** drop-down list, select **Passport.**

4 Save your changes.

NTLM authentication will now be performed on HTTP connections that match the rule.

Enabling NTLM authentication for a version 8.x firewall

Perform these steps to enable NTLM authentication for HTTP traffic.

1 Select **Policy | Access Control Rules.**

- If you are creating a new rule, click **New Rule,** then fill in the Name, Source, and Destination areas.
- If you are modifying an existing rule, select the rule, then click **Modify**.

2 Under Applications, select or verify the HTTP proxy service the rule will use.

The **Default ports** that allow HTTP and HTTPS are 80 and 443 . Select **Override ports** if you require ports other than the default ports.

Note: McAfee recommends the non-transparent HTTP (NT-HTTP) connection type. If your rule allows transparent HTTP and HTTPS connections, users must visit a non-encrypted site (HTTP) before visiting encrypted sites (HTTPS).

3 From the **Authenticator** drop-down list, select **<None/Passport>**.

4 Under Source, click **Users and Groups.**

5 Click the **Groups** tab and select the <**Authenticated>** checkbox.

6 Click **OK** and save your changes.

NTLM authentication will now be performed on HTTP connections that match the rule.

Configuring the users' browsers

To configure users' browsers to perform Integrated Windows Authentication with Firewall Enterprise, perform the appropriate procedure.

- *Configuring Microsoft Internet Explorer®* on page 10
- *Configuring Mozilla Firefox®* on page 11

Configuring Microsoft Internet Explorer®

To configure Microsoft Internet Explorer, perform the following steps.

Note: This procedure is valid for Microsoft Internet Explorer version 6 or later.

1 From the **Tools** menu, select **Internet Options**. The Internet Options window appears.

2 Add the firewall IP address to the Local intranet zone.

a Click the **Security** tab.

b Select **Local intranet**, then click **Sites**. A pop-up window appears.

c Click **Advanced**. An additional pop-up window appears.

d In the **Add this website to the zone** field, type **https://*firewall_IP***, where *firewall_IP* is the firewall IP address that the domain routes traffic to.

e Click **Add**. The firewall IP address is added to the list of Local intranet websites.

f Close the pop-up windows until you return to the Security tab on the Internet Options window.

3 Modify security settings for the Local intranet zone.

   a On the Security tab, click **Custom level**. The Security Settings – Local Intranet Zone window appears.

   b Under Miscellaneous, enable the **Allow META REFRESH** option.

   c Under User Authentication, select one of the following options:

   - Automatic logon only in Intranet zone
   - Automatic logon with current use name and password

   d Click **OK** to close the Security Settings – Local Intranet Zone window.

4 Modify security settings for the Internet zone.

   a Select **Internet**, then click **Custom level**. The Security Settings – Internet Zone window appears.

   b Under Miscellaneous, enable the **Allow META REFRESH** option.

   c Click **OK** to close the Security Settings – Internet Zone window.

5 Enable the transparent authentication option.

   a Click the **Advanced** tab.

   b Under Security, select **Enable Integrated Windows Authentication**.

   Tip: You must scroll down to see this option.

   c Click **OK** to close the Internet Options window.

   d Restart Internet Explorer.

Configuring Mozilla Firefox®

To configure Mozilla Firefox, perform the following steps.

Note: This procedure is valid for Mozilla Firefox version 1.0 or later.

1 Start Firefox.

2 In the address bar, type **about:config**, then press **Enter**.

3 In the **Filter** field, type **ntlm**. The search results appear.

4 Double-click **network.automatic-ntlm-auth.trusted-uris**. The Enter string value window appears.

5 Type the IP address of the firewall, then click **OK**.

6 Restart Firefox.

Appendix

This section covers additional issues related to NTLM. The following topics are included:

Configuring McAfee SmartFilter and NTLM

Firewall Enterprise can work together with McAfee SmartFilter to control users' Internet access by performing content filtering. When NTLM authentication is used in the firewall rules that allow users' web traffic, SmartFilter supports using Active Directory groups in the SmartFilter policy.

Requirements

Before configuring Firewall Enterprise and SmartFilter to share group information, make sure you have completed the following:

- Firewall Enterprise:
  - Enabled and configured SmartFilter
  - Configured the firewall to use the same Windows Domain Controller as SmartFilter

    Note: The Windows DC must have an LDAP directory populated with the appropriate user groups.
- SmartFilter:
  - Installed and configured the SmartFilter Admin Console and SmartFilter Admin Server

    Note: If you plan to allow some users override privileges, also install and configure the SmartFilter Authentication Server.
  - Configured SmartFilter to point to the same Windows DC that the Firewall Enterprise points to

    Note: The Windows DC must have an LDAP directory populated with the appropriate user groups.
  - Created the SmartFilter policies that you will assign to the user groups

SmartFilter and Firewall Enterprise configuration

1. In the SmartFilter Admin Console, add the LDAP directory.
   a. In the top panel, select **Enterprise Settings**.
   b. In the lower panel, select **Directory Resources**.
   c. Click **Add**, then configure the following fields:
      - In the **Name** field, enter the host name of your domain controller.
      - In the **Address** field, enter the host name or IP address of your domain controller.
      - From the **Type** drop-down list, select **Active Directory**.
      - Select **Allow Windows NTLM Authentication**.
   d. Click **Auto Config**. A pop-up window appears.
   e. In the pop-up window, enter your directory credentials, then click **OK**. Another pop-up window appears.
   f. In the pop-up window, select the path that contains the SmartFilter groups the firewall will use, then click **Select**. You return to the Directory Resources window.
   g. Click **OK**. The domain controller is added to the list of directory resources.

2 Add the LDAP directory to the appropriate firewall plugin.

   a In the top panel, select **Individual Plugins**, then select the firewall plugin.

   b In the bottom panel, select **Apply Policies | Configure Groups | Directories**.

   c Move the LDAP directory from the right-hand area to the left-hand area.

   d If you have more than one directory listed, position them in the order SmartFilter should search them.

   e Click **OK**. A confirmation window appears.

   f Click **Yes**.

3 Match each user group to a SmartFilter policy.

   a In the bottom panel, select **Apply Policies | Group Policies**.

   b Click **Add**.

   c Use the **Search Directories** button (...) to look up groups on the LDAP directory.

   d For each group, select the appropriate policy, then click **OK**.

4 In the toolbar, click the **Download Control List** icon to obtain the latest control list.

5 Deploy your changes to the firewall plugin.

6 On the Firewall Enterprise, find the rule you created or modified in *Adding NTLM authentication to rules* on page 9. Make sure that SmartFilter is enabled on the rule's Application Defense.

7 Save your changes.

Your Firewall Enterprise now filters web traffic according to the assigned SmartFilter policy and Active Directory groups.

Granting users SmartFilter override capabilities

You may want to allow some users to override SmartFilter policy. Follow this procedure to grant override privileges to users that require them.

Note: To follow this procedure, you must have the SmartFilter Authentication Server installed.

1 In the SmartFilter Admin Console, add the LDAP directory to the SmartFilter Authentication Server.

   a In the top panel, select **Authentication Servers**, then select the authentication server.

   b In the lower panel, select **Authentication Directories**.

   c Move the LDAP directory from the right-hand area to the left-hand area.

   d If you have more than one directory listed, position them in the order SmartFilter should search them.

   e Click **OK**.

2 Select the SmartFilter Authentication Server on the firewall plugin.

   a In the top panel, select **Individual Plugins**, then select the firewall plugin.

   b In the lower panel, select **Set Advanced Options | Authentication**. Ensure that the authentication server is selected from the **SmartFilter Authentication Server** drop-down list.

   c Click **OK**.

3 Configure override accounts.

   a In the bottom panel, select **Apply Policies | Overrides**.

   b Click **Add**.

c Use the **Search Directories** button (...) to browse to the LDAP directory containing the user groups to be used with the firewall.

d Find each user that requires override capabilities, and add their name to the list.

e Click **OK**.

4 Deploy your changes to the firewall plugin.

Avoiding certificate errors

Most modern browsers examine SSL certificates presented to them to ensure they are valid and trusted. Passport presents an SSL certificate to users' browsers when authentication takes place.

Issues to address

You may need to address some or all of the following issues to avoid certificate errors during Passport authentication:

- The Passport certificate must be signed by a Certificate Authority (CA) that is trusted by the browser.

  For details, see the "Certificate/Key Management" chapter of the *McAfee*® Firewall Enterprise *Administration Guide*.

- The Common Name (CN) used in the Distinguished Name (DN) of the Passport certificate must match the host name of the firewall.

  For details, see the "Certificate/Key Management" chapter of the *McAfee*® Firewall Enterprise *Administration Guide*.

- The client (browser) must be able to resolve the firewall's host name to the IP address of the firewall in the same zone using DNS.

- Passport must be configured to redirect authentication sessions to the host name of the firewall rather than its IP address.

By default, Passport uses a self-signed SSL certificate. To satisfy the conditions above, you may need to create or import a new certificate for use with Passport. To select a different Passport certificate, go to **Policy | Application Defenses | Defenses | HTTPS | Passport**, and select the desired certificate from the **Firewall certificate** drop-down list.

Configuring Passport to redirect to a host name

By default, Passport redirects authentication sessions to the firewall IP address in the same zone as the client. This may cause certificate warnings, since many web browsers compare the redirect destination to the host name in the SSL certificate presented by Passport. To avoid these errors, you can configure Passport to redirect authentication sessions to the firewall's host name.

Note: Your firewall must be at version 7.0.0.05 or later to redirect Passport sessions to a host name.

To configure Passport to redirect to a host name, edit the httpp.conf file, then restart the HTTP and HTTPS proxies.

1 Open the httpp.conf file.

   a In the Admin Console, go to **Maintenance | File Editor**, then click **Start File Editor** in the right pane. The File Editor window appears.

   b From the **File** menu, select **Open**. The Open File window appears.

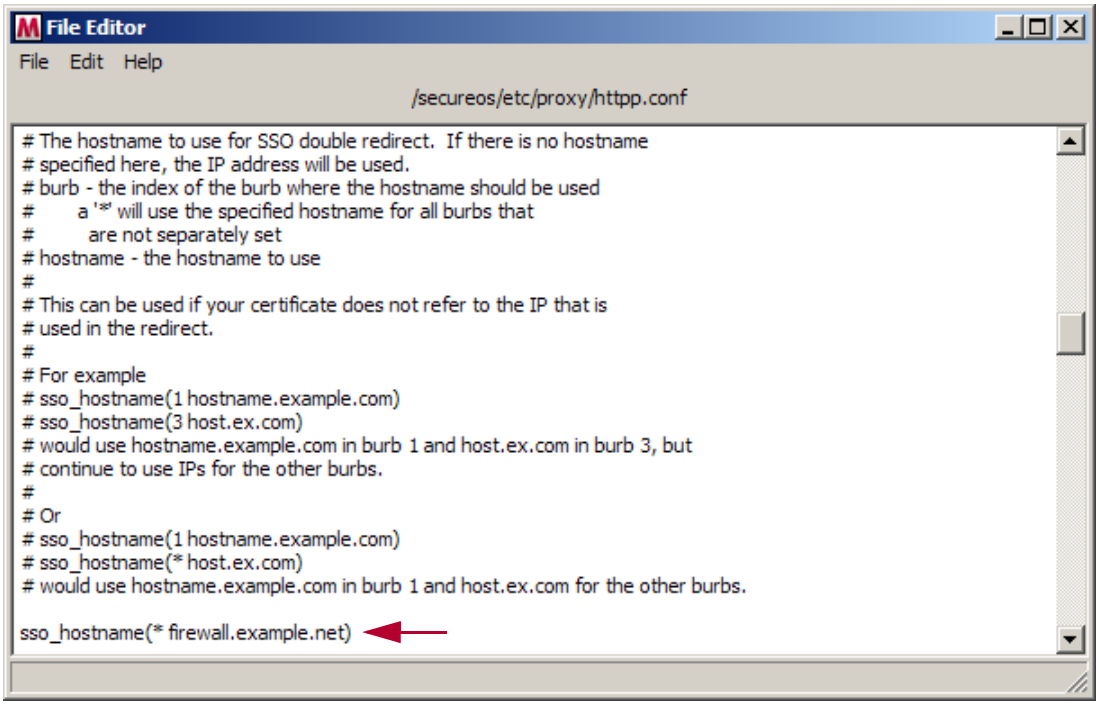
   c In the **Source** field, select **Firewall File**.

   d In the **File** field, type **/secureos/etc/proxy/httpp.conf**, then click **OK**. The httpp.conf file opens in the File Editor.

2 Edit the httpp.conf file.

   a Scroll down to the SSO host name comments section.

   Figure 2 Example configuration change



   b After the SSO comments, type the following:

   `sso_hostname(* firewall_hostname)`

   where *firewall_hostname* is the firewall host name.

   Note: This modification affects Passport redirection for all zones. You can also configure the redirection behavior on a per-zone basis. See the comments in httpp.conf for details.

   c Save your changes, then close the File Editor.

3 Restart the HTTP and HTTPS proxies.

   a Select **Monitor | Service Status**. The Service Status window appears.

   b To restart the HTTP proxy, right-click **http** in the Service list, then select **Restart**.

   c To restart the HTTPS proxy, right-click **https** in the Service list, then select **Restart**.

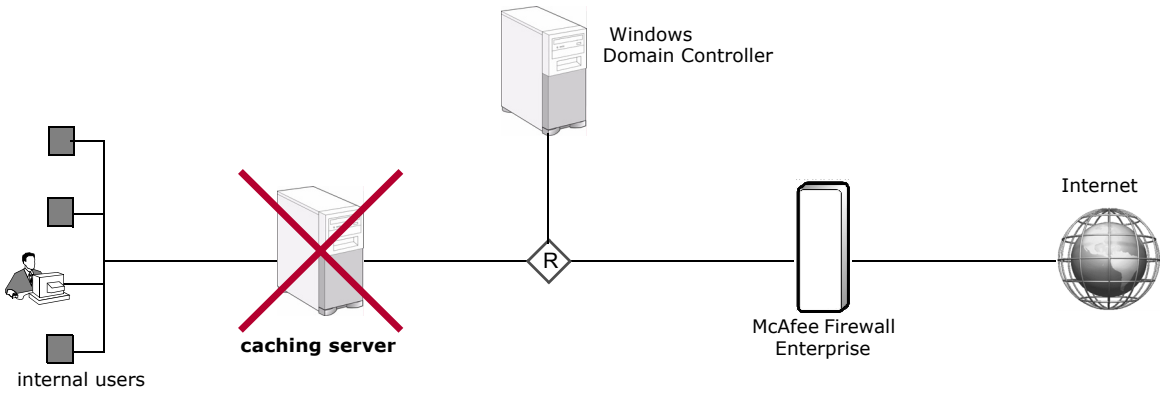
   Tip: If either proxy is not running, it will not appear in the list of services. The changes you made will take effect when the proxy is enabled.

Passport will now redirect authentication sessions to the host name you specified in httpp.conf.

Avoiding unsupported configurations

NTLM sees each connection as a single person. If you have a caching device set up between your internal users and your firewall, the caching device will present one connection on behalf of all users. This configuration will not accurately authenticate users and can cause problems. This configuration is unsupported.

Figure 3 Unsupported caching configuration



Using a caching server on the external side of the firewall does not cause the same problem.