TECHNICAL NOTE
STORMSHIELD NETWORK SECURITY

CONFIGURING "GUEST" AUTHENTICATION METHODS

Product concerned : SNS 3.0 and higher versions

Document version : 1.0

Reference : sns-en-configuring_guests_modes_technical-note

Table of contents

Before we begin

In order for an organization's external users to access certain network resources (Internet access, for example), version 3 of SNS firmware offers three authentication methods:

- Guest mode (declaratory mode): this method is based on the user's acceptance of a disclaimer setting out Internet access conditions. It is particularly suited to public Internet access in high-traffic areas such as restaurants, railway stations or libraries.
- Temporary accounts: limited-duration accounts can be created, with a configurable validity period for each account. This method is ideal, for example, for hotel infrastructures that wish to offer Internet access only for the duration of a client's stay.
- Sponsorship method: on the captive portal, the user enters his first and last names and the email address of an internal sponsor. If this internal sponsor is authorized and has been explicitly declared on the firewall as being allowed to sponsor users, he will then confirm the request, immediately granting the requester access to web resources. This method may be used in organizations, for example, to provide visiting service providers with Internet access.

Configuring the Guest method (declaratory mode)

Basically, this mode consists of identification without authentication. During the user's initial connection to the Internet, he will be redirected to the captive portal. He will then be shown the conditions of use for Internet access, which he must accept in order to access the requested website. Next, depending on the URL filter policy implemented, the user will then be able to access web resources. Conditions of use will regularly reappear; the frequency of their display can be configured. Guest users' connections are valid for 4 hours.

Up to three complementary fields can be added (e.g., first name, last name, email address, etc.) for the guest user to fill in before accepting the conditions of use. This additional information will be reflected in the firewall's log files. Several authentication profiles can also be defined for the captive portal. For every profile that can be associated with one or several network interfaces on the firewall, several Internet access authorizations can be configured using Guest mode with different parameters (complementary fields) that depend on the interface from which the user connects.

Enabling Guest method

1. In the *Available methods* tab in the **Users** > **Authentication** module, expand the **Add a method** menu and select **Guest**.
2. In the panel on the right, adjust the display frequency of the Conditions of use for Internet access This frequency may be expressed in minutes, hours or days. The default value is 1440 minutes (18 hours).

Creating rules in the authentication policy

1. In the *Authentication policy* tab in the **Users** > **Authentication** module, expand the **New rule** menu and select **Guest rule**.
2. Click on **Add an interface** and select the interface(s) from which guest accounts may be created.
3. Click on **Add an object** to select (or create then select) the network or hosts from which guest users will log on.
4. Confirm by clicking on **Finish**.
5. Double click on the status of the rule to enable it.
6. Click on **Apply**.

Customizing captive portal profiles for the Guest method

In the *Captive portal profiles* tab in the **Users** > **Authentication** module, select the "Guest" profile.

This profile will automatically implement the parameters needed for this method to run:

Authentication

- **Default method or directory:** *"Guests (guest_users.local.domain)"*.

Conditions of use for Internet access

- **Enable the display of the conditions of use for Internet access** The frequency with which these conditions are displayed has been set to 18 hours.

> **NOTE**
> The text contained in the conditions of use can be customized in the *Captive portal* tab.

Customized fields on the captive portal

- **Field no. 1**: E-mail address
- **Field no. 2**: Empty
- **Field no. 3:** Empty

> **NOTE**
>
> These fields are optional and do not necessarily need to be filled out to accept the conditions of use.

Advanced properties

- **Enable the captive portal.**
- **Expiry of the HTTP cookie**: *"At the end of the authentication period".*

If any of these parameters have been modified (e.g.: customized fields on the captive portal), click on **Apply** to save the configuration.

Mapping the captive portal's profile to the affected network interfaces

Select the *Captive portal* tab in the **Users > Authentication** module. The **Authentication profile and interface match** table is empty. Click on **Add** to selected the desired interface and assign the *Guest* profile to it. The method and directory associated with this profile will automatically appear in the *Default method or directory* column:

> **NOTE: firewalls that have been migrated from a 2.x version to a 3.x version**
>
> 1. Select the *Captive portal* tab in the **Users > Authentication** module. The **Authentication profile and interface match** table suggests the firewall's interfaces by default and associates them with *External* profiles for unprotected interfaces and *Internal* profiles for protected interfaces.
> 2. On the same row as the desired interface, click inside the **Profile** column and select the associated profile (*Guest* in the example). The domain name associated with the profile will be automatically indicated.

Adapting the filter policy for guest users

The filter policy described below allows guest users to access websites in HTTP and HTTPS with URL filtering.

Creating an SSL inspection rule

Two rules can be created in the wizard: one to decrypt HTTPS traffic and the other to direct such traffic to the SSL proxy so that it can be analyzed by URL filter rules and intrusion prevention processes.

1. In the *Filtering* tab in the **Security policy** > **Filter - NAT** module, click on **New rule** and select **SSL inspection rule**.
2. Enter details about the source networks or hosts (**From** column - *guests_network* in the example), the destination (**To** column - *Internet* in the example) and the destination port (*HTTPS* in the example). Confirm by clicking on **Finish**.
3. Double click on the source of the rule that redirects to the SSL proxy. In the **User** field, select Any user@guest_users.local.domain.
4. In the *Advanced properties* tab, select *Guest* as the **Authentication method**.
5. In **Port / Protocol**, select *Application protocol* for the **Protocol type** field, then *HTTP* for the **Application protocol**.
6. In **Inspection**, select the URL filter profile to apply (*URLFilter_00* in the example),
7. Confirm by clicking on **OK**.

Creating a captive portal redirection rule

1. In the *Filtering* tab in the **Security policy** > **Filter - NAT** module, click on **New rule** and select **Authentication rule**.
2. In the wizard, enter the source networks or hosts (**From** field - *guests_network* in the example) and the destination (**To** field - *Internet* in the example) for which unauthenticated users will be redirected to the captive portal.
3. Confirm by clicking on **Finish**. This rule selects the HTTP port as the default destination port.
4. To add the HTTPS port to it, double click on the **Dest. port** field in this rule. In the **Destination port** field in the window where rules are edited, click on **Add an object** ( ) and select the HTTPS port. Confirm by clicking on **OK**.
5. Using the **Up** and **Down** arrows, position this rule between the SSL decryption rule and the SSL proxy redirection rule.

Adding HTTP traffic filter rules for guest users

1. In the *Filtering* tab in the **Security policy** module, click on **New rule** and select **Single rule**.
2. In the Status column, double-click on *Off* to enable the rule (the status of the rule becomes *On*).
3. In the **Action** column, double-click on *block* then select the value *pass* for the **Action** field: Select the desired log level for connections that match this rule; *log (filter log)* makes it possible to view events relating to the connections of guest users in connection logs, for example.
4. In the **Source** section located to the left of the rule editing window, assign the following values to the various fields:

General tab

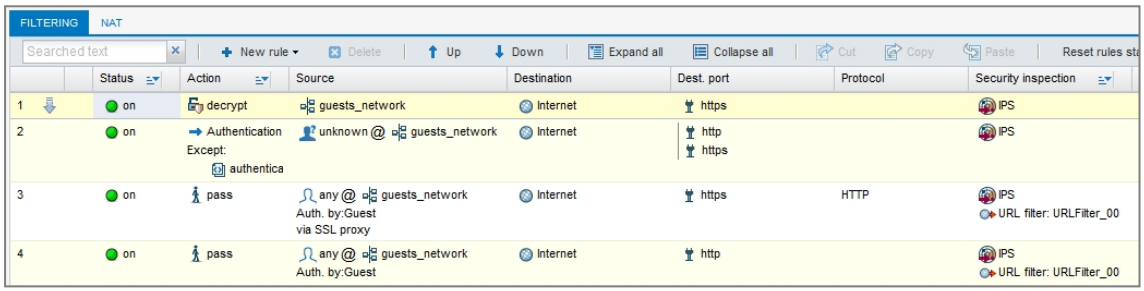
- **User**: select *Any user@guest_users.local.domain.*
- **Source hosts**: select the guest user network.

Advanced properties tab

- **Authentication method**: select the *Guest* method

5. In the **Destination** section, select the *Internet* object for the **Destination hosts** field
6. In the **Port / Protocol** section, select the HTTP object for the **Destination port** field
7. In **Inspection**, leave the IPS mode suggested by default and select the URL filter profile to apply (*URLFilter_00* in the example), This profile can be customized in the **Security policy > URL filtering** menu.

The filter policy regarding guest users will therefore resemble the following:



Viewing logs

In the *Guest* method, users are not saved in an LDAP directory. Instead, they are associated with accounts automatically generated by the firewall with lifetimes that match guest users' authentication durations.

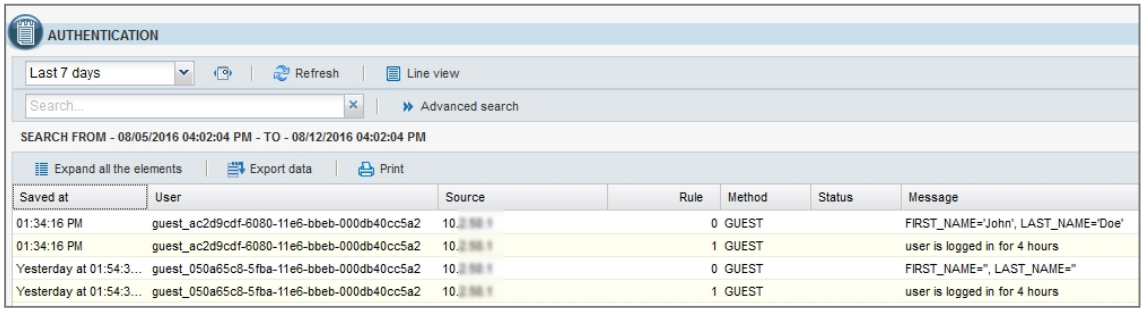
These accounts take on the form of a random character string with a "guest_" prefix.

If customized first name, last name and email address fields, for example, have been defined in the authentication profile, the values entered in these fields will make it possible to associate the real user with the virtual user.

Mapping the virtual account to complementary information

In the firewall's web administration interface, look up logs (**Authentication, Network connections** and **Filter**) and reports in order to check that the implemented configuration is running as planned.

The Authentication log indicates the *guest_xxxx* name assigned by the firewall (**User** column), the host's source IP address, the method ("Guest") and the value of any additional fields if the user has filled them in (**Message** column).



Configuring the Temporary account method

In this method, limited-duration accounts can be created. Such accounts comprise at least a first name and a last name that make up the account identifier, as well as an automatically generated password. The validity period of these accounts can be configured for each account. This method is ideal, for example, for hotel infrastructures that wish to offer Internet access only for the duration of a client's stay.

The creation of temporary accounts can be delegated to users who have access restricted exclusively to the module that allows them to create such accounts.

Enabling the Temporary account method

1. In the *Configuration* tab in the **Users > Temporary accounts** module, select the **Enable temporary accounts module** checkbox.
2. You can set a default validity period (expressed in days) when creating a new account.

   NOTE

   Every time a new account is created, this period will be suggested by default and can be replaced with a customized duration.
3. Apply changes. The Temporary accounts method will then be automatically added to the list of available authentication methods.

Adding a user delegated with the creation of temporary accounts

If you wish to delegate the creation of temporary accounts to one or several users, temporary account administrators must be defined. Whenever they log on to the firewall administration interface, these particular users will only have access to the temporary account management module.

1. In **System > Administrators**, expand the **Add an administrator** menu and select **Add an administrator for temporary accounts**.
2. Select an existing user. This user must come from the firewall's internal LDAP.
3. Confirm the creation of the user by clicking on **Apply**.

Creating rules in the authentication policy

1. In the *Authentication policy* tab in the **Users > Authentication** module, expand the **New rule** menu and select **Temporary accoun rule**.
2. Click on **Add an interface** and select the network interface from which guest accounts may be created.
3. Click on **Add an object** to select (or create then select) the network or hosts from which guest users will log on.
4. Confirm by clicking on **Finish**.
5. Double click on the status of the rule to enable it.
6. Click on **Apply**.

Customizing captive portal profiles for the Guest method

In the *Captive portal profiles* tab in the **Users** > **Authentication** module, select the "Voucher" profile.

This profile will automatically implement the parameters needed for this method to run:

Authentication

- **Default method or directory:** *"Temporary accounts(voucher_users.local.domain)"*.

Authentication periods allowed

- **Minimum duration**: may be set from 1 minute to 24 hours (value suggested by default: 15 minutes).
- **Maximum duration**: may be set from 1 minute to 24 hours (value suggested by default: 4 hours).

Advanced properties

- **Enable the captive portal.**
- **Expiry of the HTTP cookie**: *"At the end of the authentication period"*.

Complementary settings:

Conditions of use for Internet access

Select the **Enable the display of the conditions of use for Internet access** checkbox if you want these conditions to be shown whenever a user logs on. They will also be displayed at a regular interval (value suggested by default: 18 hours).

NOTE
The text contained in the conditions of use can be customized in the *Captive portal* tab.

If any of these parameters have been modified (e.g.: authentication periods), click on **Apply** to save the configuration.

Mapping the captive portal's profile to the affected network interfaces

Select the *Captive portal* tab in the **Users** > **Authentication** module. The **Authentication profile and interface match** table is empty. Click on **Add** to selected the desired interface and assign the *Voucher* profile to it. The method and directory associated with this profile will automatically appear in the *Default method or directory* column:

NOTE: firewalls that have been migrated from a 2.x version to a 3.x version

1. Select the *Captive portal* tab in the **Users** > **Authentication** module. The **Authentication profile and interface match** table suggests the firewall's interfaces by default and associates them with *External* profiles for unprotected interfaces and *Internal* profiles for protected interfaces.

2. On the same row as the desired interface, click inside the **Profile** column and select the associated profile (*Voucher* in the example). The domain name associated with the profile will be automatically indicated.

Adapting the filter policy for temporary account users

The filter policy described below allows temporary account users to access websites in HTTP and HTTPS with URL filtering.

Creating an SSL inspection rule

Two rules can be created in the wizard: one to decrypt HTTPS traffic and the other to direct such traffic to the SSL proxy so that it can be analyzed by URL filter rules and intrusion prevention processes.

1. In the *Filtering* tab in the **Security policy > Filter - NAT** module, click on **New rule** and select **SSL inspection rule**.
2. Enter details about the source networks or hosts (**From** column - *temporary_accounts_network* in the example), the destination (**To** column - *Internet* in the example) and the destination port (*HTTPS* in the example). Confirm by clicking on **Finish**.
3. Double click on the source of the rule that redirects to the SSL proxy. In the **User** field, select Any user@voucher_users.local.domain.
4. In the *Advanced properties* tab, select Temporary accounts as the **Authentication method**.
5. In **Port / Protocol**, select *Application protocol* for the **Protocol type** field, then *HTTP* for the **Application protocol**.
6. In **Inspection**, select the URL filter profile to apply (*URLFilter_00* in the example),
7. Confirm by clicking on **OK**.

Creating a captive portal redirection rule

1. In the *Filtering* tab in the **Security policy > Filter - NAT** module, click on **New rule** and select **Authentication rule**.
2. In the wizard, enter the source networks or hosts (**From** field - *guests_network* in the example) and the destination (**To** field - *Internet* in the example) for which unauthenticated users will be redirected to the captive portal.
3. Confirm by clicking on **Finish**. This rule selects the HTTP port as the default destination port.
4. To add the HTTPS port to it, double click on the **Dest. port** field in this rule. In the **Destination port** field in the window where rules are edited, click on **Add an object** ( ) and select the HTTPS port. Confirm by clicking on **OK**.
5. Using the **Up** and **Down** arrows, position this rule between the SSL decryption rule and the SSL proxy redirection rule.

Adding HTTP traffic filter rules for temporary accounts

1. In the *Filtering* tab in the **Security policy** module, click on **New rule** and select **Single rule**.
2. In the Status column, double-click on *Off* to enable the rule (the status of the rule becomes *On*).

3. In the **Action** column, double-click on *block* then select the value *pass* for the **Action** field: Select the desired log level for connections that match this rule; *log (filter log)* makes it possible to view events relating to the connections of temporary accounts in connection logs, for example.
4. In the **Source** section located to the left of the rule editing window, assign the following values to the various fields:

General tab

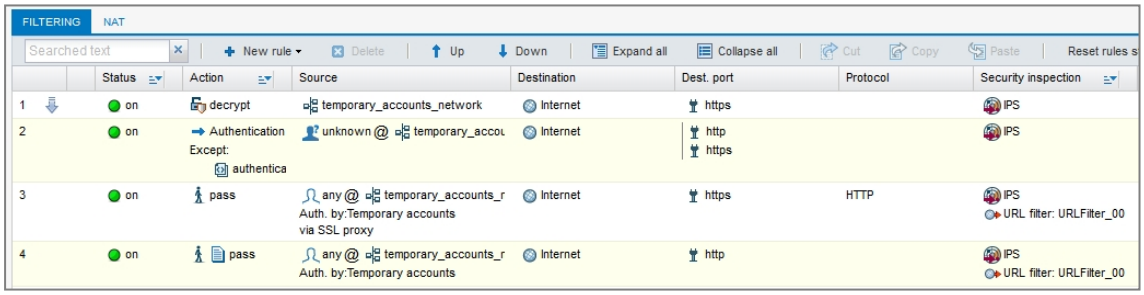
- **User**: select *Any user@voucher_users.local.domain.*
- **Source hosts**: select the temporary account network.

Advanced properties tab

- **Authentication method**: select the *Temporary accounts* method

5. In the **Destination** section, select the *Internet* object for the **Destination hosts** field
6. In the **Port / Protocol** section, select the HTTP object for the **Destination port** field
7. In **Inspection**, leave the IPS mode suggested by default and select the URL filter profile to apply (*URLFilter_00* in the example), This profile can be customized in the **Security policy > URL filtering** menu.

The filter policy regarding temporary accounts will therefore resemble the following:



Viewing logs

In the firewall's web administration interface, look up logs (**Authentication, Network connections** and **Filter**) and reports in order to check that the implemented configuration is running as planned.

Configuring the Sponsorship method

In this mode, shared Internet access can be granted to service providers visiting the organization's premises. During his initial connection to the Internet, the user will be redirected to the captive portal on which he can submit his request for sponsorship by indicating his first and last names and the email address of an internal sponsor. If this internal sponsor is authorized and has been explicitly declared on the firewall as being allowed to sponsor users, he will then confirm the request, immediately granting the requester access to web resources.

He will then be shown the conditions of use for Internet access, which he must accept in order to access the requested website. Next, depending on the URL filter policy implemented, the user will then be able to access web resources. Conditions of use will regularly reappear; the frequency of their display can be configured. Guest users' connections are valid for 4 hours. After this period is up, the Conditions of use for Internet access will automatically be displayed.

Configuring sponsorship emails

Defining the mail server

1. In the *Configuration* tab in the **Notifications > Email alerts** module, select the **Enable e-mail notifications** checkbox.
2. **Server** field: select or create the host network object corresponding to the mail server.
3. **Port** field: select the mail server's listening port (in general, SMTP or SMTPS).
4. If the connection to the mail server requires authentication, fill in the **Login** and **Password** fields.
5. **DNS domain** field: enter the mail domain name. It will be attached to the name of the firewall in order to form a valid sender email address.
6. Confirm by clicking on **Apply**.

Customizing the sponsorship email (optional)

1. In the *Templates* tab in the **Notifications** > **Email alerts** module, select the **Sponsorship request** e-mail (**Sponsorship** section).
2. Click on **Modify** if you wish to customize the email that is sent whenever a sponsorship request is received then save your changes.

Enabling the Sponsorship method

1. In the *Available methods* tab in the **Users > Authentication** module, expand the **Add a method** menu and select Sponsorship.
2. In the panel on the right, set the minimum and maximum authentication periods. The respective values suggested by default are 15 minutes and 4 hours.

Allowing users to validate sponsorship requests

Define a user or user group authorized to validate sponsorship requests received by email.

1. Select the *Detailed access* tab in the **Users > Access privileges** module.
2. Click on **Add** to add a new line to the table of privileges (none will be assigned).
3. Click on **User - user group** and select an existing user or user group. This user or group must come from the firewall's internal LDAP.
4. Click on the **Sponsorship** field and select *Allow*.
5. Double click on the **Status** column in order to enable this privilege rule.
6. Confirm the creation of the user by clicking on **Apply**.

Creating rules in the authentication policy

1. In the *Authentication policy* tab in the **Users > Authentication** module, expand the **New rule** menu and select **Sponsorship rule**.
2. Click on **Add an interface** to select the network interface from which sponsorship requests may be sent.
3. Click on **Add an object** to select (or create then select) the network or hosts from which guest users will log on.
4. Confirm by clicking on **Finish**.
5. Double click on the status of the rule to enable it.
6. Click on **Apply**.

Customizing captive portal profiles for the Guest method

In the *Captive portal profiles* tab in the **Users > Authentication** module, select the "*Sponsor*" profile.

The following parameters will be implemented directly with this profile:

Authentication

- **Default method or directory:** *"Sponsorship (sponsored_users.local.domain)"*.

Authentication periods allowed

- **Minimum duration**: may be set from 1 minute to 24 hours (value suggested by default: 15 minutes).
- **Maximum duration**: may be set from 1 minute to 24 hours (value suggested by default: 4 hours).

Advanced properties

- **Enable the captive portal.**
- **Expiry of the HTTP cookie:** "**None**".

IMPORTANT

The cookie timeout parameter in particular must not be modified for the Sponsorship method.

Moreover, the fact that cookies are not used will prohibit the use of multi-user objects (TSE servers for example) as source hosts for this method.

Complementary settings:

Conditions of use for Internet access

Select the **Enable the display of the conditions of use for Internet access** checkbox if you want these conditions to be shown whenever a user logs on. They will also be displayed at a regular interval (value suggested by default: 18 hours).

NOTE
The text contained in the conditions of use can be customized in the *Captive portal* tab.

If any of these parameters have been modified (e.g.: authentication periods), click on **Apply** to save the configuration.

Mapping the captive portal's profile to the affected network interfaces

Select the *Captive portal* tab in the **Users > Authentication** module. The **Authentication profile and interface match** table is empty. Click on **Add** to selected the desired interface and assign the *Sponsor* profile to it. The method and directory associated with this profile will automatically appear in the *Default method or directory* column:

NOTE: firewalls that have been migrated from a 2.x version to a 3.x version

1. Select the *Captive portal* tab in the **Users > Authentication** module. The **Authentication profile and interface match** table suggests the firewall's interfaces by default and associates them with *External* profiles for unprotected interfaces and *Internal* profiles for protected interfaces.
2. On the same row as the desired interface, click inside the **Profile** column and select the associated profile (*Sponsor* in the example). The domain name associated with the profile will be automatically indicated.

Adapting the filter policy for temporary account users

The filter policy described below allows sponsored users to access websites in HTTP and HTTPS with URL filtering.

Creating an SSL inspection rule

Two rules can be created in the wizard: one to decrypt HTTPS traffic and the other to redirect such traffic to the SSL proxy so that it can be analyzed by URL filter rules and intrusion prevention processes.

1. In the *Filtering* tab in the **Security policy > Filter - NAT** module, click on **New rule** and select **SSL inspection rule**.
2. Enter details about the source networks or hosts (**From** column - *sponsorship_network* in the example), the destination (**To** column - *Internet* in the example) and the destination port (*HTTPS* in the example). Confirm by clicking on **Finish**.

3. Double click on the source of the rule that redirects to the SSL proxy. In the **User** field, select Any user@sponsored_users.local.domain.
4. In the *Advanced properties* tab, select *Sponsorship* as the **Authentication method**.
5. In **Port / Protocol**, select *Application protocol* for the **Protocol type** field, then *HTTP* for the **Application protocol**.
6. In **Inspection**, select the URL filter profile to apply (*URLFilter_00* in the example),
7. Confirm by clicking on **OK**.

Creating a captive portal redirection rule

1. In the *Filtering* tab in the **Security policy > Filter - NAT** module, click on **New rule** and select **Authentication rule**.
2. In the wizard, enter the source networks or hosts (**From** field - *sponsorship_network* in the example) and the destination (**To** field - *Internet* in the example) for which unauthenticated users will be redirected to the captive portal.
3. Confirm by clicking on **Finish**. This rule selects the HTTP port as the default destination port.
4. To add the HTTPS port to it, double click on the **Dest. port** field in this rule. In the **Destination port** field in the window where rules are edited, click on **Add an object** ( ) and select the HTTPS port. Confirm by clicking on **OK**.
5. Using the **Up** and **Down** arrows, position this rule between the SSL decryption rule and the SSL proxy redirection rule.

Adding HTTP traffic filter rules for sponsored users

1. In the *Filtering* tab in the **Security policy** module, click on **New rule** and select **Single rule**.
2. In the Status column, double-click on *Off* to enable the rule (the status of the rule becomes *On*).
3. In the **Action** column, double-click on *block* then select the value *pass* for the **Action** field: Select the desired log level for connections that match this rule; *log (filter log)* makes it possible to view events relating to the connections of sponsored users in connection logs, for example.
4. In the **Source** section located to the left of the rule editing window, assign the following values to the various fields:

General tab

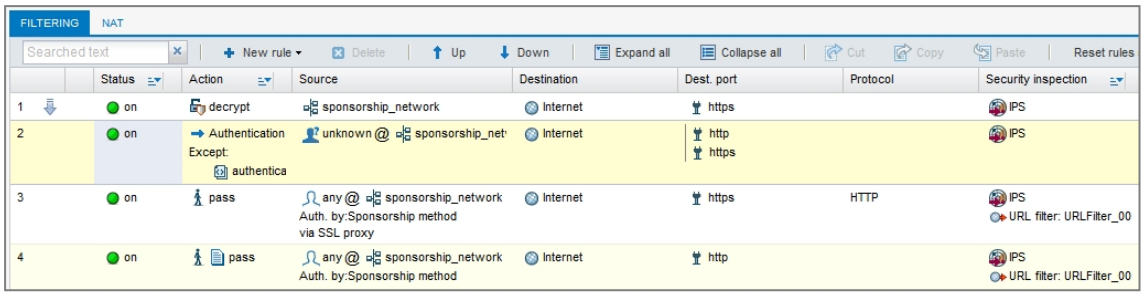
- **User**: select *Any user@sponsored_users.local.domain.*
- **Source hosts**: select the temporary account network.

Advanced properties tab

- **Authentication method**: select the *Temporary accounts* method

5. In the **Destination** section, select the *Internet* object for the **Destination hosts** field
6. In the **Port / Protocol** section, select the HTTP object for the **Destination port** field
7. In **Inspection**, leave the IPS mode suggested by default and select the URL filter profile to apply (*URLFilter_00* in the example), This profile can be customized in the **Security policy > URL filtering** menu.

The filter policy regarding sponsored users will therefore resemble the following:



Viewing logs

In the firewall's web administration interface, look up logs (**Authentication, Network connections** and **Filter**) and reports in order to check that the implemented configuration is running as planned.