Astaro Security Gateway V7

Software version: 7.000 or higher

Site-to-Site VPN via RSA

Configuring ASG

Author: Richard Striegel
Contact: documentation@astaro.com
Document version: 1.000
Date: 2007-03-15
Status: Public

Contents **Page**

1. Introduction

The guides contain complementary information on the Administration Guide and the Online Help. If you are not sure whether you have the current version of this guide, you can download it from the following Internet address:

http://www.astaro.com/kb

If you have questions or find errors in the guide, please, contact us under the following e-mail address:

documentation@astaro.com

For further help use our support-forum under ...

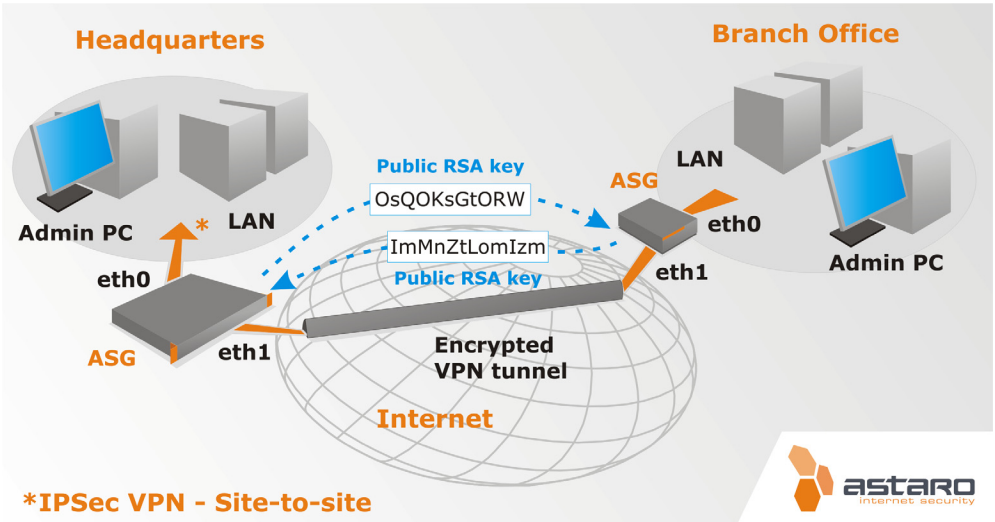
http://www.astaro.com

... or use the Astaro Support offers ...

http://www.astaro.com/support

2. Site-to-site VPN Connection via RSA

This chapter describes step by step the configuration of an **Site-to-site VPN** connection between two **Astaro Security Gateways** by using **RSA keys**. An IPSec VPN tunnel allows for example a secure data traffic between a headquarters office and a branch office. One Astaro Security Gateway serves as Internet gateway in the headquarters and the branch office respectively.



The structure is described in the left chart: In both systems the network card **eth1/LAN** is connected to the Internet and the network card **eth0 /WAN** to the local network.

First ensure to have the following information available:

- Local gateway (Host name or IP address)
- Local network (IP address)
- Remote gateway (Host name or IP address)
- Remote network (IP address)

2.1. Background Information

RSA Keys

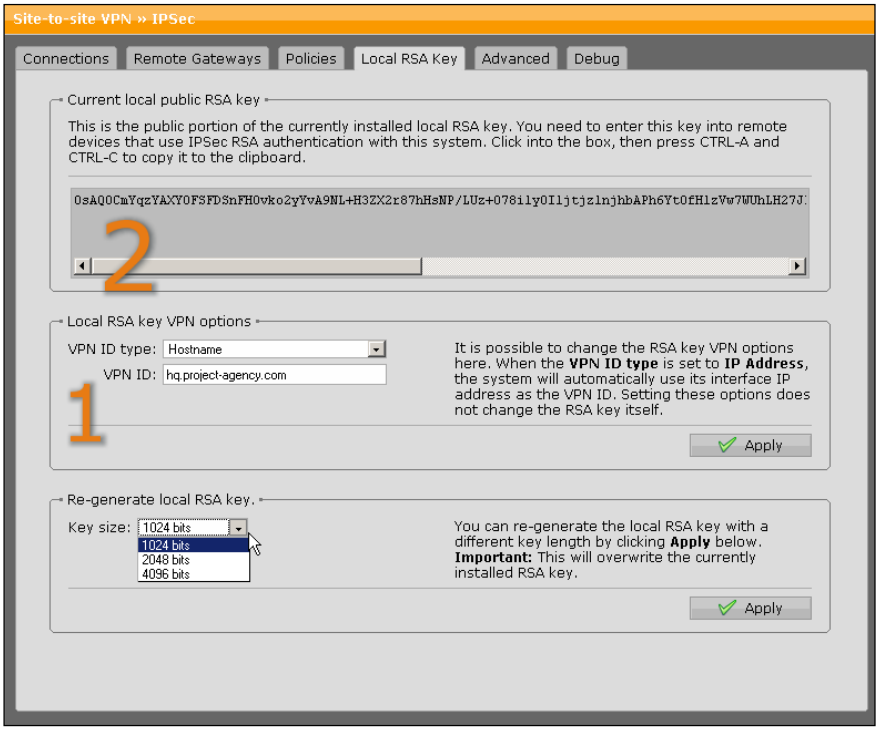
The authentication via **RSA** is made with **public keys** and **private keys**. The *private key* must remain secret, whereas the *public key* (see chart on page 2) may be transmitted via the Internet. During the definition of the *private key*, a *public key* is created on both sides of the IPSec tunnel. This *public key* will then be imported to the other side of the tunnel.
Both keys are mathematically dependent from each other and are in a unique relation to each other: Data, which had been encrypted with one *key* can only be decrypted with the corresponding key on the remote endpoint. It requires important efforts to deduct the *private key* from the *public key*. If you use the Internet to access the remote security system from your local network, you may exchange the keys via the clipboard.

2.2. Configuration of the local VPN Gateway

The Astaro Security Gateway is configured via the web based **WebAdmin** interface from the administration PC. Opening and using this configuration tool is extensively described in the **Astaro Security Gateway V7** administration guide.

1. Retrieve the local RSA key:

Open the **Site-to-Site VPN >> IPSec >> Local RSA Key** tab.



When the *Astaro Security Gateway* is started the first time, the **Local RSA key VPN** options (screenshot: Item 1) are preset and an RSA key (screenshot: Item 2) is automatically created by using the random number generator.

You can also regenerate the local RSA key with another key length, but that isn't necessary.

Set the local RSA key VPN options:

VPN ID type: A unique identifier must be indicated for each VPN gateway. Select the identifier type and enter the value as described below into the **VPN ID** dialog box:

Hostname: Select this type for a VPN gateway with static IP address or when the dynamic IP address is resolved through DynDNS. The host name is preset in the **VPN ID** dialog box (in this example: *hq.project-agency.com*).

Optional VPN identifier types:

IP address: This identifier type is useful for a VPN gateway with static IP address. Enter the appropriate IP address in the **VPN ID** dialog box.

Email address: Enter the e-mail address of the local VPN gateway administrator.

Confirm your settings by clicking **Apply**.

Now, regenerate the local RSA key:

Key size: Select the key size.

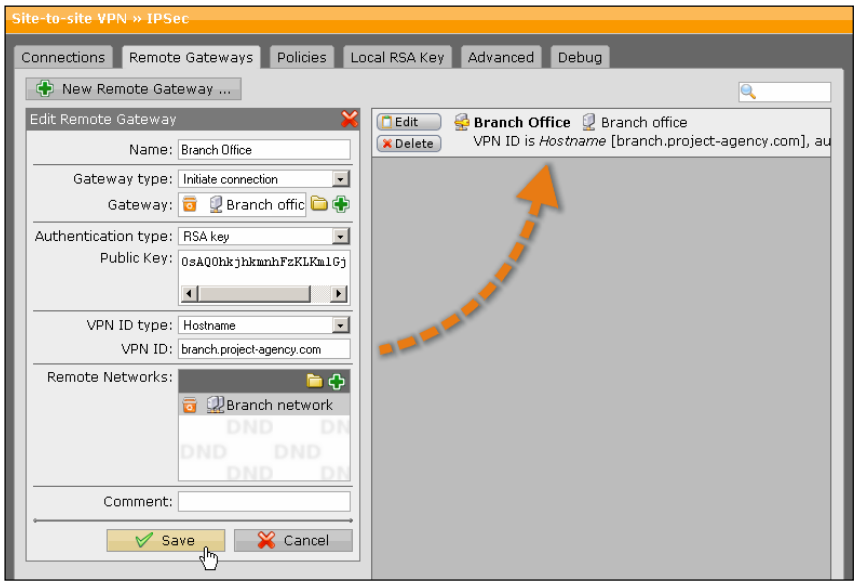
Security Note:

To enhance security set a key size of at least 2048 bits. The length of the RSA key (RSA key size) must be the same on both VPN gateways.

Start the action by clicking **Apply**.

Depending on the hardware used and on the key size, the key generation may take a couple of minutes. The generated key will be displayed in the **Current local public RSA key** dialog box. Copy the key to the clipboard or send it per e-mail to the administrator of the remote VPN gateway.

2. *Define the remote gateway (static/dynamic IP address):*



To configure the Site-to-site VPN connection, the required networks of the remote endpoint must be defined first. You can define networks on the **Definitions >> Networks** page or as described below on the **Site-to-site VPN >> IPSec >> Remote Gateways** tab.

Name: Enter a specific name for the remote gateway (in this example: *Branch Office*).

Gateway type: Set the remote VPN gateway type here. For a static IP address or if the remote interface is resolved through DynDNS, select **Initiate connection**. Afterwards, create the network (host) object in the **Gateway** dialog box (in this example: *Branch office*). If the IP address of the remote VPN gateway changes and is not resolved through DynDNS select **Respond only**.

For an interface with dynamic IP address (Modem/DSL) using **Dynamic DNS** you can indicate the DNS name instead of the IP address. For the DynDNS service under *www.dyndns.org* this name could be **company.dynalias.org** for example.

The **Dynamic DNS** function is described in the **Astaro Security Gateway** administration guide.

Authentication type: Select **RSA key**.

Public key: Copy the public key, which you have received from the administrator of the remote VPN gateway administrator.

Note:
Ensure that the **public key** is fully copied into the window. Already a space character at the end of the key might cause that setting up the IPSec VPN tunnel fails.

VPN ID type: Select the identifier type (in this example: *Hostname*) and enter the value in the **VPN ID** dialog box (in this example: *branch.project-agency.com*). The same VPN identifier must be configured on the remote VPN gateway on the **Local RSA Key** tab!

The optional VPN identifier types are described in step 1.

Remote networks: Select the remote networks that should be part of the VPN (in this example: *Branch network*).

Comment (optional): Add a description or other information about the remote gateway.

Confirm your settings by clicking on **Save**.

The new remote gateway will be displayed in the table.

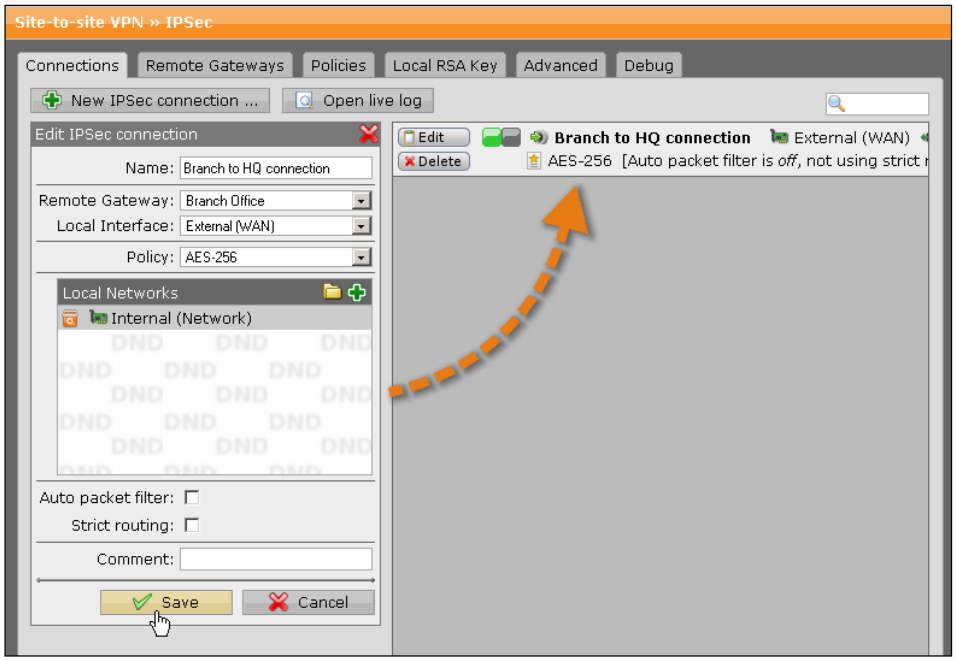
More detailed information on the configuration of a **Remote Gateway** and detailed explanations of the individual settings can be found in the **Astaro Security Gateway V7** administration guide in chapter 12.

3. *Configure the IPSec VPN connection:*

Open the **Site-to-Site VPN >> IPSec** page.

On the **Connections** tab, click **New IPSec connection**.

The **Add IPSec connection** dialog box opens.



More detailed information on the configuration of a **Site-to-Site VPN** and detailed explanations of the individual settings can be found in the **Astaro Security Gateway V7** administration guide in chapter 12.

Name: Enter a descriptive name for this connection.

Remote Gateway: Select the remote VPN gateway of the remote Astaro Security Gateway. This VPN gateway has been defined in step 2 (in this example: *Branch Office*).

Local Interface: Select the network interface to use for IPSec access (in this example: *External (WAN)*).

Policy: Select an already defined policy (in this example: **AES-256**).

You can use the **IPSec >> Policies** tab to define your own policies. Creating of own **IPSec Policies** is described in the **Astaro Security Gateway V7** administration guide in chapter 12.

Local Networks: Select the local networks that should be part of the VPN (in this example: *Internal (Network)*).

Note:

If you wish the IPSec connected users to be allowed to access the Internet, you need to select **Any** in the **Local networks** dialog box. Additionally, you need to define appropriate **Masquerading** or **NAT** rules.

Auto packet filter: Enable this option if you wish to automatically set the packet filter rules, to allow all traffic through the tunnel.

Strict routing: Enable this option in order to have the source and destination address checked whether they match the tunnel definition. Otherwise, only the destination address (remote network) is checked.
Enabling *strict routing* allows you to send both encrypted and unencrypted traffic to the same remote network, depending on the source address. Disabling this option allows the usage of SNAT rules on VPN tunnels. With SNAT rules, you can add other local networks to the same VPN tunnel, without the need to create an additional tunnel.

Comment (optional): Add a description or other information about the IPSec VPN connection.

4. Configure the advanced Site-to-Site IPSec VPN settings:

Open the **Site-to-Site VPN >> IPSec >> Advanced** tab.

| Dead Peer Detection (DPD)

The *Dead Peer Detection* option is used to automatically determine whether a remote IPSec peer can still be reached. Usually it is safe to always enable this option. The IPSec peers automatically determine whether the remote side supports *Dead Peer Detection* or not, and will fall back to normal mode if necessary.

| Misc settings

Copy TOS (Type of Service) value: **Type-of-Service**-Bits are four Bit flags in the IP header. The Bits are referred to as *Type-of-Service*-Bits, as they allow the transferring application, to tell the network which type of service quality is necessary. The available service quality classes are: minimum delay, maximum throughput, maximum reliability and minimum cost. This option copies the content of the *TOS* field in the encrypted data packet, so that the IPSec data traffic can be routed according to its priority.

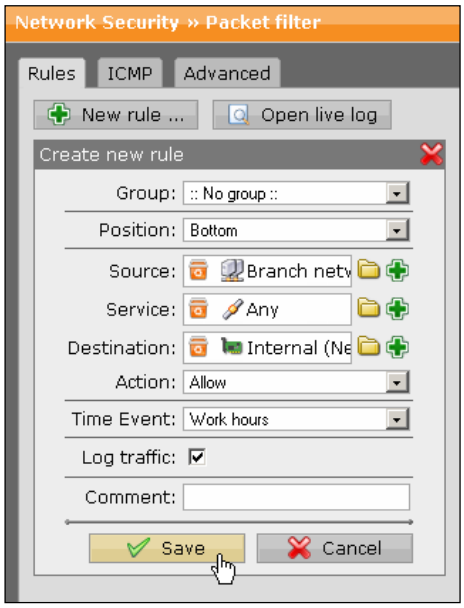
Allow path MTU discovery: It is usually preferable that IP data packets be of the largest size that does not require fragmentation anywhere along the path from the source to the destination. This size of the data packet across a connection is referred to as the *Path*

Maximum Transmission Unit (*PMTU*). If any of the data packets are too large to be forwarded without fragmentation by some router along the path, that router will discard them and return ICMP Destination Unreachable messages with a code meaning "fragmentation needed and DF set". Upon receipt of such a message, the source host reduces its assumed PMTU for the path. Enabling the *Allow path MTU discovery* option makes the ASG appliance to send such ICMP messages.

MTU: In this field you can specify the *Maximum Transmission Unit* (*MTU*) of the IPSec interface; the default MTU is 1420 byte.

5. *Define the packet filter rule (optional):*

You must define this packet filter rule if you have disabled the **Automatic packet filter rule** function during the configuration of the IPSec VPN connection in step 3.



Open the **Network Security >> Packet Filter >> Rules** tab.

After clicking on the **New rule** button the dialog box for new rules will appear. Create a new rule for the access to the local internal network.

Source: Select the remote network or user (in this example: *Branch network*).

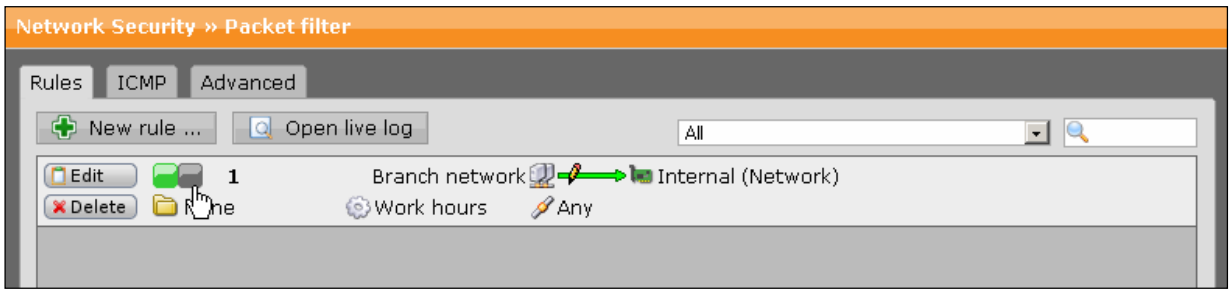
Service: Set the service (e.g. *Any* for all services).

Destination: Select the allowed internal network (in this example: *Internal (Network)*).

Action: Allow.

Confirm your settings by clicking on **Save**.

New rules will be added at the end of the list and remain disabled (status light shows red) until they are explicitly enabled by clicking on the status light.



Active rules are processed in the order of the numbers (next to the status light) until the first matching rule. Then the following rules will be ignored! The sequence of the rules is thus very important. Therefore never place a rule such as **Any** – **Any** – **Any** – **Allow** at the beginning of the rules since all traffic will be allowed through and the following rules ignored!

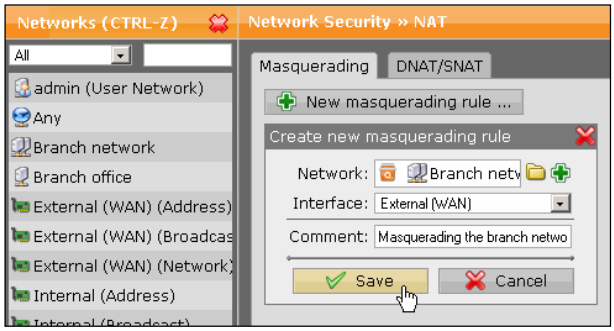
More detailed information on the definition of **Packet Filter Rules** and detailed explanations of the individual settings can be found in the **Astaro Security Gateway V7** administration guide in chapter 7.

6. *Define the masquerading rule (optional):*

Masquerading is used to mask the IP addresses of one network (in this example: *Branch Office Marketing*) with the IP address of a second network (in this example: *External*). Thus remote users, who have only private IP addresses can surf on the Internet with an official IP address.

More detailed information on the definition of **Masquerading Rules** and detailed explanations of the individual settings can be found in the **Astaro Security Gateway V7** administration guide in chapter 7.

Open the **Network Security >> NAT >> Masquerading** tab.



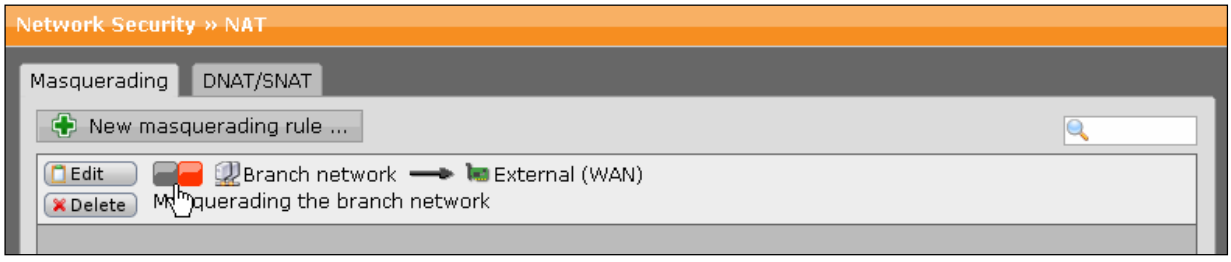
Make the following settings:

Network: Select the network of the remote endpoint (in this example: *Branch network*).

Interface: Select the interface that shall be used to mask the remote network. (in this example: *External (WAN)*).

Then confirm your settings by clicking on **Save**.

New masquerading rules will be added at the end of the list and remain disabled (status light shows red) until they are explicitly enabled by clicking on the status light.



7. *Activate the proxies (optional):*

If the remote employees shall access URL services via the remote access you may configure the required proxies on the Astaro Security Gateway – this would be the **DNS** and **HTTP proxy** for example.

More detailed information on the configuration of **Proxies** and detailed explanations of the individual settings can be found in the **Astaro Security Gateway V7** administration guide.

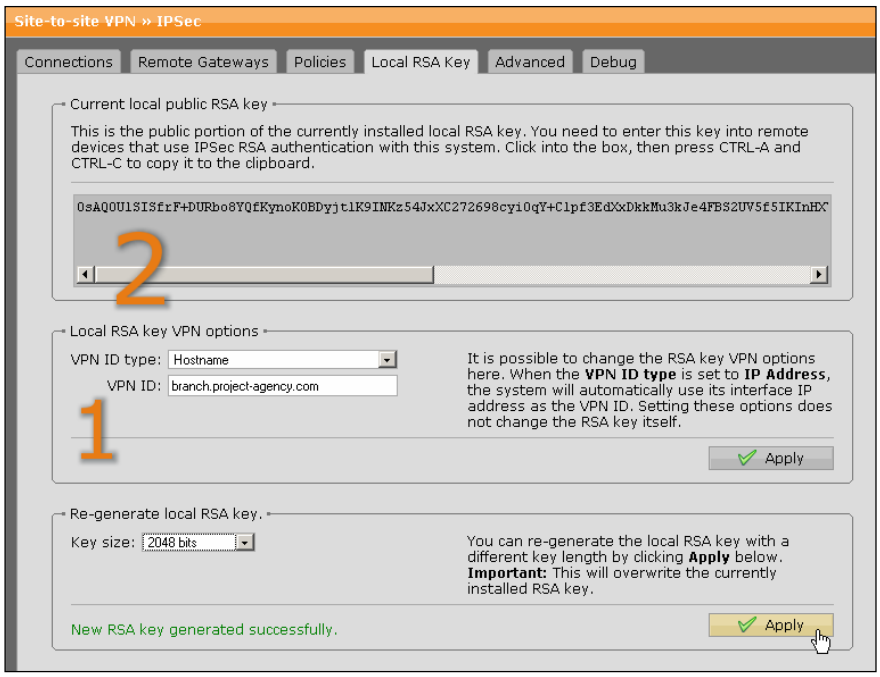
After configuring the VPN server (Headquarters) you must configure the remote VPN gateway (Branch Office). The basic settings for the VPN IPSec tunnel are now finished. Depending on the Security Policy of your organization and the requirements of your network you might have to make additional settings.

2.3. Configuration of the remote VPN Gateway

After configuring the VPN server (Headquarters) you must configure the remote Astaro Security Gateway (Branch Office).

1. *Retrieve the local RSA key:*

Open the **Site-to-Site VPN >> IPSec >> Local RSA Key** tab.



When the *Astaro Security Gateway* is started the first time, the **Local RSA key VPN** options (screenshot: Item 1) are preset and an RSA key (screenshot: Item 2) is automatically created by using the random number generator.

You can also regenerate the local RSA key with another key length, but that isn't necessary.

Set the local RSA key VPN options:

VPN ID type: A unique identifier must be indicated for each VPN gateway. Select the identifier type and enter the value as described below into the **VPN ID** dialog box:

Hostname: Select this type for a VPN gateway with static IP address or when the dynamic IP address is resolved through DynDNS. The host name is preset in the **VPN ID** dialog box (in this example: *branch.project-agency.com*).

Optional VPN identifier types:

IP address: This identifier type is useful for a VPN gateway with static IP address. Enter the appropriate IP address in the **VPN ID** dialog box.

Email address: Enter the e-mail address of the local VPN gateway administrator.

Confirm your settings by clicking **Apply**.

Now, regenerate the local RSA key:

Key size: Select the key size.

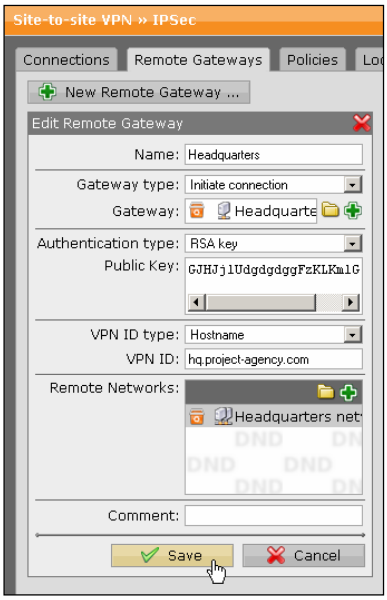
Security Note:

To enhance security set a key size of at least 2048 bits. The length of the RSA key (RSA key size) must be the same on both VPN gateways.

Start the action by clicking **Apply**.

Depending on the hardware used and on the key size, the key generation may take a couple of minutes. The generated key will be displayed in the **Current local public RSA key** dialog box. Copy the key to the clipboard or send it per e-mail to the administrator of the remote VPN gateway.

2. *Define the remote gateway (static/dynamic IP address):*



To configure the Site-to-site VPN connection, the required networks of the remote endpoint must be defined first. You can define networks on the **Definitions >> Networks** page or as described below on the **Site-to-site VPN >> IPSec >> Remote Gateways** tab.

Name: Enter a specific name for the remote gateway (in this example: *Headquarters*).

Gateway type: Set the remote VPN gateway type here. For a static IP address or if the remote interface is resolved through DynDNS, select **Initiate connection**. Afterwards, create the network (host) object in the **Gateway** dialog box (here: *Headquarters*). If the IP address of the remote VPN

gateway changes and is not resolved through DynDNS select **Respond only**.

For an interface with dynamic IP address (Modem/DSL) using **Dynamic DNS** you can indicate the DNS name instead of the IP address. For the DynDNS service under *www.dyndns.org* this name could be **company.dynalias.org** for example.

The **Dynamic DNS** function is described in the **Astaro Security Gateway** administration guide.

Authentication type: Select **RSA key**.

Public key: Copy the public key, which you have received from the administrator of the remote VPN gateway administrator.

Note:

Ensure that the **public key** is fully copied into the window. Already a space character at the end of the key might cause that setting up the IPSec VPN tunnel fails.

VPN ID type: Select the identifier type (in this example: *Hostname*) and enter the value in the **VPN ID** dialog box (in this example: *hq.project-agency.com*). The same VPN identifier must be configured on the remote VPN gateway on the **Local RSA Key** tab!

The optional VPN identifier types are described in step 1.

Remote networks: Select the remote networks that should be part of the VPN (in this example: *Headquarters network*).

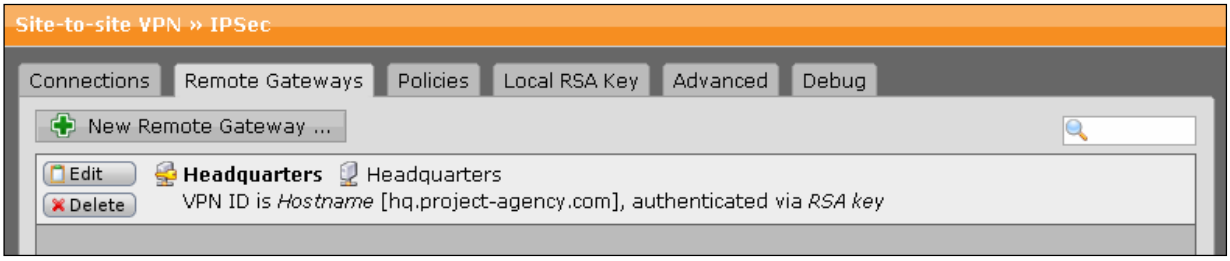
Note:

If you wish the local users to be allowed to access the Internet via the remote Astaro Security Gateway, you need to select **Any** in the **Remote networks** dialog box.

Comment (optional): Add a description or other information about the remote gateway.

Confirm your settings by clicking on **Save**.

The new remote gateway will be displayed in the table.



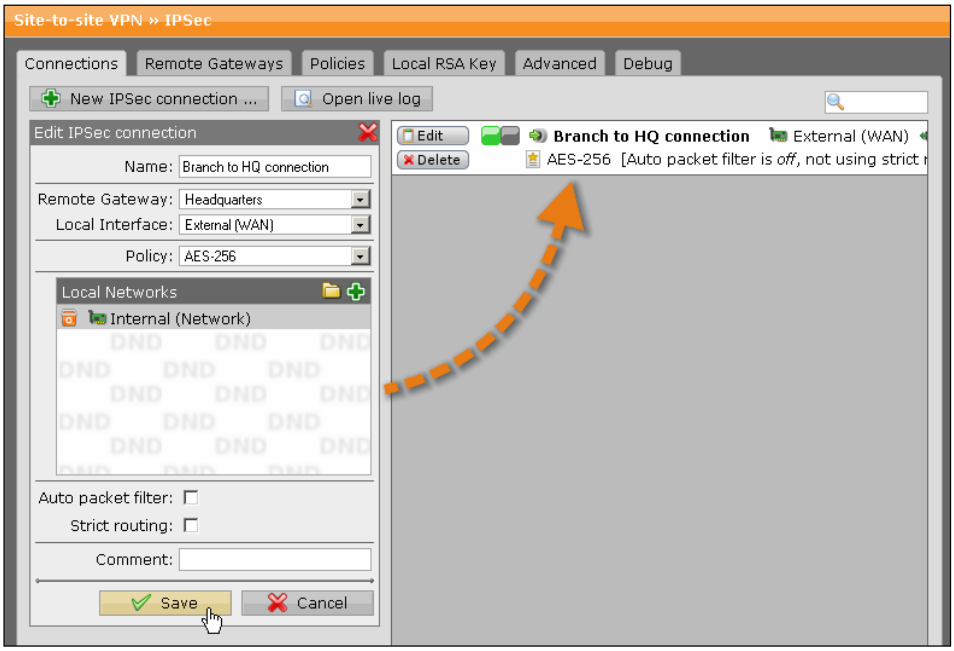
More detailed information on the configuration of a **Remote Gateway** and detailed explanations of the individual settings can be found in the **Astaro Security Gateway V7** administration guide in chapter 12.

3. *Configure the IPSec VPN connection:*

Open the **Site-to-Site VPN >> IPSec** page.

On the **Connections** tab, click **New IPSec connection**.

The **Add IPSec connection** dialog box opens.



More detailed information on the configuration of a **Site-to-Site VPN** and detailed explanations of the individual settings can be found in the **Astaro Security Gateway V7** administration guide in chapter 12.

Name: Enter a descriptive name for this connection.

Remote Gateway: Select the remote VPN gateway of the remote Astaro Security Gateway. This VPN gateway has been defined in step 2 (in this example: *Headquarters*).

Local Interface: Select the network interface to use for IPSec access (in this example: *External (WAN)*).

Policy: Select an already defined policy (in this example: **AES-256**).

You can use the **IPSec >> Policies** tab to define your own policies. Creating of own **IPSec Policies** is described in the **Astaro Security Gateway V7** administration guide in chapter 12.

Local Networks: Select the local networks that should be part of the VPN (in this example: *Internal (Network)*).

Auto packet filter: Enable this option if you wish to automatically set the packet filter rules, to allow all traffic through the tunnel.

Strict routing: Enable this option in order to have the source and destination address checked whether they match the tunnel definition. Otherwise, only the destination address (remote network) is checked.
Enabling *strict routing* allows you to send both encrypted and unencrypted traffic to the same remote network, depending on the source address. Disabling this option allows the usage of SNAT rules on VPN tunnels. With SNAT rules, you can add other local networks to the same VPN tunnel, without the need to create an additional tunnel.

Comment (optional): Add a description or other information about the IPSec VPN connection.

4. Configure the advanced Site-to-Site IPSec VPN settings:

Open the **Site-to-Site VPN >> IPSec >> Advanced** tab.

| Dead Peer Detection (DPD)

The *Dead Peer Detection* option is used to automatically determine whether a remote IPSec peer can still be reached. Usually it is safe to always enable this option. The IPSec peers automatically determine whether the remote side supports *Dead Peer Detection* or not, and will fall back to normal mode if necessary.

| Misc settings

Copy TOS (Type of Service) value: **Type-of-Service**-Bits are four Bit flags in the IP header. The Bits are referred to as *Type-of-Service*-Bits, as they allow the transferring application, to tell the network which type of service quality is necessary. The available service quality classes are: minimum delay, maximum throughput, maximum reliability and minimum cost. This option copies the content of the *TOS* field in the encrypted data packet, so that the IPSec data traffic can be routed according to its priority.

Allow path MTU discovery: It is usually preferable that IP data packets be of the largest size that does not require fragmentation anywhere along the path from the source to the

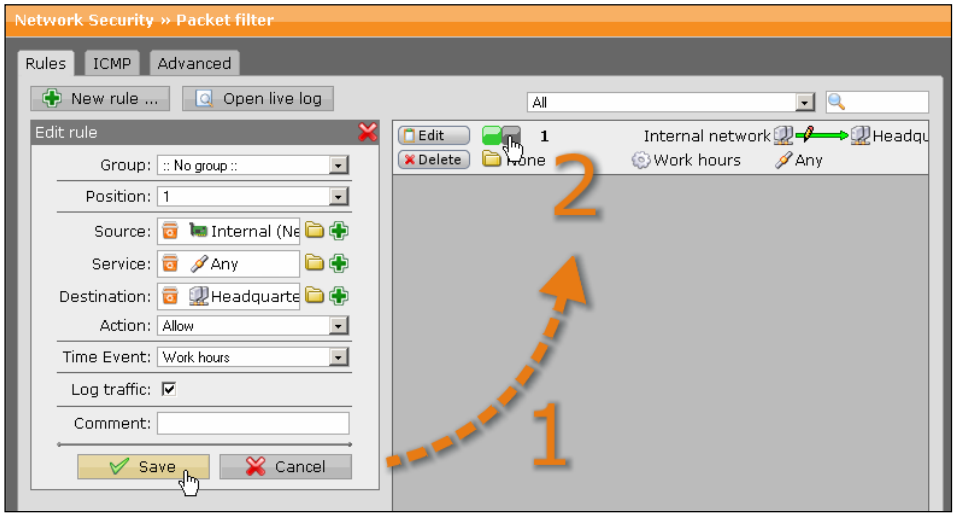
destination. This size of the data packet across a connection is referred to as the *Path Maximum Transmission Unit* (*PMTU*). If any of the data packets are too large to be forwarded without fragmentation by some router along the path, that router will discard them and return ICMP Destination Unreachable messages with a code meaning "fragmentation needed and DF set". Upon receipt of such a message, the source host reduces its assumed PMTU for the path. Enabling the *Allow path MTU discovery* option makes the ASG appliance to send such ICMP messages.

MTU: In this field you can specify the *Maximum Transmission Unit* (*MTU*) of the IPSec interface; the default MTU is 1420 byte.

5. *Define the packet filter rule (optional):*

You must define this packet filter rule if you have disabled the **Automatic packet filter rule** function during the configuration of the IPSec VPN connection in step 3.

Open the **Network Security >> Packet Filter >> Rules** tab.



After clicking on the **New rule** button the dialog box for new rules will appear. Create a new rule for the access to the local internal network.

Source: Select the local network or user (in this example: *Internal (Network)*).

Service: Set the service (e.g. *Any* for all services).

Destination: Select the allowed internal network (in this example: *Headquarters*).

Action: Allow.

Confirm your settings by clicking on **Save**.

New rules will be added at the end of the list (see screenshot: Item 1) and remain disabled (status light shows red) until they are explicitly enabled by clicking (see screenshot: Item 2) on the status light.

Active rules are processed in the order of the numbers (next to the status light) until the first matching rule. Then the following rules will be ignored! The sequence of the rules is thus very important. Therefore never place a rule such as **Any** – **Any** – **Any** – **Allow** at the beginning of the rules since all traffic will be allowed through and the following rules ignored!

More detailed information on the definition of **Packet Filter Rules** and detailed explanations of the individual settings can be found in the **Astaro Security Gateway V7** administration guide in chapter 7.

6. Activate the proxies (optional):

If the remote employees shall access URL services via the IPSec VPN tunnel you may configure the required proxies on the security system – this would be the **DNS** and **HTTP proxy** for example.
Depending on the configuration you create a proxy-chain by defining the proxy of the headquarters as **upstream proxy** of the branch office. This applies to both, the HTTP and the DNS proxy.

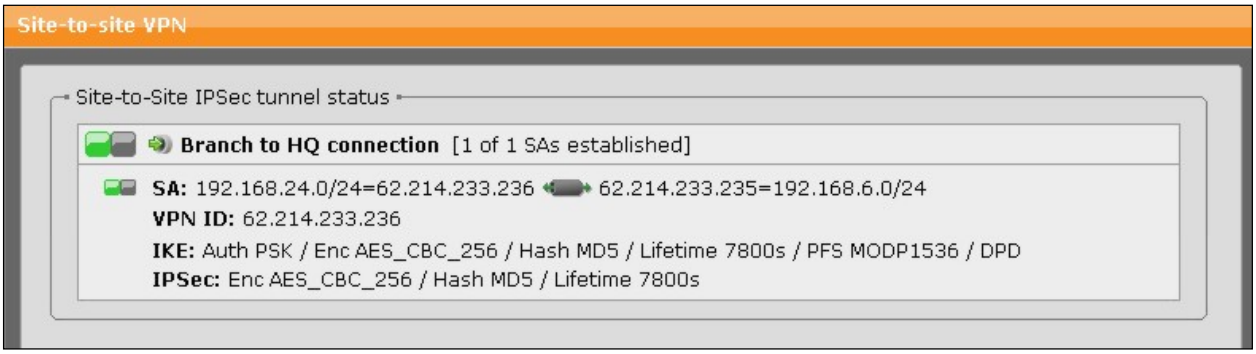
More detailed information on the configuration of **Proxies** and detailed explanations of the individual settings can be found in the **Astaro Security Gateway V7** administration guide.

The basic settings for the VPN IPSec tunnel are now finished. Depending on the security policy of your organization and the requirements of your network you might have to make additional settings.

3. Maintenance Functions

IPSec Connection Status

The **Site-to-site VPN** page contains the **Site-to-site IPSec Tunnel Status** overiew. This displays all currently negotiated or established IPSec VPN connections. A connection is then fully established, when the status lights of the accordant IPSec tunnel are both green. The table contains the following messages:



Connection Name: The name for the IPSec VPN connection.

SA: Indicates the IPSec SA status: red = inactive, yellow = being negotiated, green = set-up.

VPN ID: The remote *VPN ID* (if no IP address) and the current IP address of the receiver.

IKE: This line displays the **Internet Key Exchange (IKE)** protocol settings.

IPSec: This line displays the **IPSec tunnel** settings.

Error: This line is shown if the connection isn't established yet.