

NETASQ

MIGRATING FROM V8 TO V9

Document version: 1.1

Reference: naentno_migration-v8-to-v9

INTRODUCTION	3
Upgrading on a production site	3
Compatibility	3
Requirements	4
Accessing the firewall after the upgrade	4
MAIN CHANGES IN VERSION 9	5
Web management interface	5
Protecting access to the GUI	5
Filter and NAT policy	6
IPS inspection	7
IPSec VPN	7
User directory	7
GENERAL POINTS REGARDING MIGRATION	8
Configuration modules retained	8
Reinitialization	9
Partially retained modules	9
Status of the configuration modules after the upgrade	10
MIGRATING THE FILTER POLICY	11
Typical order of a migrated policy	11
Compatibility of V8 and V9 filter rules	13
MIGRATING THE NAT POLICY	14
Main points	14
Map 15	
Nomap	16
Bi-directional map (bimap)	16
Redirection (rdr)	17
Redirection with load balancing (split)	17
NAT on non-TCP/UDP/ICMP protocols (Example: GRE)	18
NAT option in the IPSec tunnel	19
End of the double assessment of the policy	19
MIGRATING THE IPSEC VPN POLICY	20
Mobile users	20
Migrating the PKI	21

Introduction

The aim of this document is to provide as much information as possible in order to allow migrating a V8 configuration to V9.

WARNING

Version 9 involves many modifications as well as profound conceptual changes. As such, the configuration upgrade process could not be fully automated.

Upgrading on a production site

Since upgrades to version 9 are not fully automated, you are advised against upgrading directly on the production site without first defining the configuration in V9. As a matter of fact, resetting to the default configuration for some modules may cause interruptions to services during upgrades.

To minimize the possibility of service interruptions, it is therefore recommended that you prepare the upgrade to version 9 with a virtual image, and then create a backup of this configuration, in order to restore it on the operational appliance.

To ease the migration, a virtual image and a license will be provisioned in the client areas.

Compatibility

Hardware platforms

The upgrade to version 9 is compatible with all U-Series and NG-Series appliances.

Operating system (firmware)

The lowest version from which you can upgrade to version 9 is version 8.0.3.

Administration suite

The version 9 administration suite is compatible with the following platforms:

- Microsoft Windows XP, Vista, Seven
- Microsoft Windows Server 2003, Server 2008, Server 2008 R2

Web management interface

The web management interface is compatible with most browsers that support JavaScript. It has been validated and maintained on the following browsers:

- Microsoft Internet Explorer, version 7 and higher
- Mozilla Firefox, version 3.6 and higher

Requirements

In order to ensure that operations run smoothly, human intervention and assistance on the site to be migrated are absolutely necessary and the following conditions have to be met:

- Lowest initial firmware version 8.0.3,
- Lowest target firmware version 9.0.4,
- Routing and access allowed in HTTPS and tcp_1300 from the remote administration workstation,
- If the firewalls are in HA, ensure that they have been correctly synchronized.

Accessing the firewall after the upgrade

In order to guarantee access to the firewall after the upgrade, the connection has to be made from the same IP address range, on port 1300/TCP (Firewall_srv) and also on port 443/TCP (HTTPS).

Main changes in version 9

This section is not meant to be a substitute for the release notes for this version, published during the release of version 9. It merely groups the significant conceptual changes you should be aware of before performing a migration.

Web management interface

NETASQ firewalls in version 9 embed a web administration interface, which will replace the “Manager” view in NETASQ Unified Manager. NETASQ firewalls can therefore be administered from a web browser.

After upgrading to version 9, the management interface will listen on TCP port 443 (HTTPS port). The administrator will be able to connect through the URL

https://<Firewall IP address>/admin/

NOTE

If there is a NAT rule in the policy to be migrated that redirects traffic from outside the firewall to another host on port 443 (HTTPS), access to the firewall’s management interface will be blocked.

This listening port can be configured in the *System > Configuration* menu, *Firewall administration* tab. In the same window, the administrator can and needs to define the list of hosts and/or networks allowed to connect to the administration page. Indeed, the same server (sld) manages the administration interface and the user portals. This list will therefore define who can view the */admin/* section.

NOTE

For architectures that combine remote administration (on the public interface) and a secure web server (HTTPS), the administrator can change the listening port of the web management interface. If he does not do so and defines a NAT operation to provide access to the internal server, it will be impossible to connect to the management interface.

Protecting access to the GUI

In version 9, access to the administration interface is protected by a software-based access control list (ACL), which can be configured in the *System > Configuration* menu, *Firewall Administration* tab.

After a migration from V8 to V9, access to the administration interface will be allowed regardless of the administration IP address. The object ‘Any’ is in fact used as a configuration setting.



ACCESS TO FIREWALL ADMINISTRATION PAGES	
+ Add a server Delete	
Authorized administration host (host or group - network - address range)	
any	

 **WARNING**

By default (defaultconfig), access to the firewall's administration interface is restricted only to hosts included in the 'Network_internals' object.

Filter and NAT policy

The filter policy can be accessed from the *Security policy > Filtering and NAT* menu. The filter policy involves many new items which are described in the document "15 Highlights of the Filter Policy". In the context of an upgrade to version 9, it is however important to understand the following information:

Common filter and NAT policy

A configuration in version 8 offers 10 separate policies for each filter and NAT module, making a total of 20 "slots".

In version 9, as the NAT and filter modules have been grouped together, 10 policies are used in common for filtering and NAT.

The filter and NAT policy is assessed in a single operation by the packet processing engine. This means in particular that the configuration, even if it is presented in two tabs, will be written in a common configuration file.

Evaluation of filtering and the impact of NAT

In version 9, **the filter policy is assessed on IP addresses before their modification via NAT**, meaning the IP addresses of the network packet before it reaches the firewall.

This modification is very important for building a proper policy. For example, in version 9, in order to allow access to an internal server from a public network (e.g. the internet), the public address of this server (or the firewall's public address, for example) has to be entered. This approach is different from version 8, which required the use of the server's private address, since the filter was assessed after the NAT operation on the destination.

 **NOTE**

The filter rule retains a similar syntax. For redirections, version 9 offers a simplified version, defined directly in the filter rule.

 **IMPORTANT**

In version 8, the most specific NAT rules are assessed as a priority.

In version 9, the execution of a rule cancels the execution of the rules that follow. The order in which rules are assessed is therefore kept.

Assessment of filtering

In version 9, rules whose action is “pass” with active explicit HTTP proxy, “decrypt” or “log” do not cancel the execution of the rules that follow. The rule assessment continues.

As such, it is possible to add filtering rules after that type of rules.

Scheduling by rule

Scheduling in version 9 is now done within filter rules and no longer by policy. Scheduling is applied within filter policies by assigning a time object in the *action* column.

NOTE

The alarm “79 - Configuration Migration: scheduling was used in V8 but is not available in V9” is generated during the migration of a policy that uses scheduling.

IPS inspection

In version 8, the *ASQ configuration* window allowed defining the firewall’s behavior in relation to the traffic that passes through it. This section also offered the configuration of alarms, signatures, quarantine, probes and plugins.

ASQ inspection profiles in version 9 are defined in the module **Application protection > Protocols and applications**. For the configuration of URL and MAIL filter rules according to profile, please refer to the respective modules in the section **Security policy**.

IPSec VPN

The IPSec VPN configuration module has been fully rewritten to simplify the configuration of tunnels. The other objective is to allow the configuration to be modified by commands instead of by sending files.

User directory

In version 9, specific attributes needed for running the firewall are stored locally. It is no longer necessary to modify the schema of an external database (Active Directory or LDAP). The result of this is that the firewall will no longer read these attributes if they are in an external database.

In the case of an internal LDAP directory, these attributes, which were necessary in version 8, will be deleted. The rest of the information (users and groups) will remain.

General points regarding migration

During the migration of a filter and NAT or VPN policy, the configuration backup in version 8 keeps only **the active slot** of each policy.

The “Global” or “Local” format has been maintained for the filter and NAT policies. IPSec VPN policies also keep their status, but only the local policy will be available in the V9 web administration interface. The Global VPN policy can be accessed via the application NETASQ Centralized Manager.

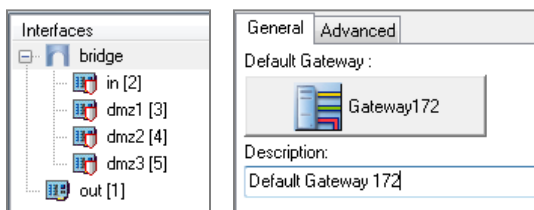
The **scheduling** feature will not be migrated as its operation mode differs in V9. Scheduling is now carried out by assigning time objects in the *action* column of a rule.

Configuration modules retained

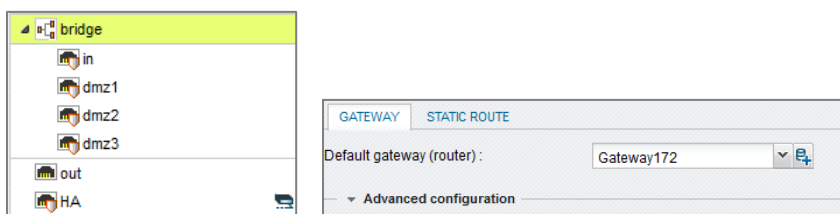
Most of the modules retain their configuration parameters as well as their statuses. To see the list of these modules, please refer to the section [Status of the configuration modules after the upgrade](#).

The migration of the **Network configuration** allows, in particular, keeping the settings of your interfaces. The upgrade also retains your **network objects** and your **user database (LDAP)**.

V8 network configuration



Network after migration to V9



Reinitialization

The modules that have been reinitialized in the default configuration are:

- **Various ASQ parameters,**
- **User pre-shared keys,**
- **URL and mail filtering,**
- **Certificates (internal PKI),**
- **Administration privileges,**
- **SSL VPN profiles,**
- **Log configuration,**
- **Secure configuration (USB).**

Partially retained modules

- **Internal user database (LDAP):**

The partial migration of an internal LDAP database can only be carried out during the upgrade of the firewall (.maj file) from version 8 to version 9. The internal LDAP directory cannot be restored from a configuration backup file (.na file).

Data that will not be migrated are all NETASQ fields, including user pre-shared key data.

- **Authentication:**

This module has been retained, only the SRP and NTLM methods have been removed.

- **Filtering:** See the chapter [Migrating the filter policy](#)
- **NAT:** See the chapter [Migrating the NAT policy](#)
- **IPSEC VPN:** See the chapter [Migrating the IPsec VPN policy](#)

Status of the configuration modules after the upgrade

	V8 configuration	Version 9.0.4
System	System / Configuration	retained
	DNS	retained
	Time zone	retained
	NTP	retained
	Administration privileges	factory settings
	Secure configuration (USB)	factory settings
	Active update	retained
Network	Network (firewall interfaces)	retained
	Routing	retained
	Dynamic routing	retained
	Dynamic DNS	retained
	DHCP server	retained
Objects	Network objects	retained with new objects added
	Customized URL groups	retained
	Imported certificates (external)	retained
	Certificates (internal PKI)	factory settings
User	LDAP (internal)	partially retained
	LDAP (external)	retained
	Authentication	retained (without SRP and NTLM methods)
	keytab (SPNEGO)	retained
Security policy	Filtering	Migrated and pending validation
	NAT	Migrated
	URL and Mail filtering	factory settings
	QoS	retained
Application protection	ASQ configuration > ASQ	factory settings except MSS limit (TCP)
	ASQ configuration > Alarms and Plugins	factory settings
	ASQ configuration > Lists	partially retained (whitelist only)
	Content analysis (Antispam, Antivirus)	Migrated
VPN	IPSEC VPN	Migrated accordingly
	Pre-shared keys	retained
	User pre-shared keys	factory settings
	SSL VPN (servers)	retained
	SSL VPN (profiles)	factory settings
	PPTP server	retained
Notifications	Log configuration	factory settings
	Syslog/SMTP (alarms)	retained
	E-mail groups	retained
	SNMP	Retained
	Events	retained
	System events	retained

Migrating the filter policy

In version 9, as the **filter policy** is applied **before translation operations on the destination**, unlike the version 8 operating mode, certain rules may cease to have the expected outcome. As a result, they are disabled by default and will need to be **modified manually**.

Some options that have not been migrated also require certain filter rules to be rewritten. These options are **ASQ inspection profiles** reinitialized in factory settings and **URL and MAIL filtering**, the format of which has been changed.

REMINDER

Migration retains only the **active slot** of the V8 configuration.

The **scheduling** feature will not be migrated. You will need to assign a time object in the *action* column of a rule in order to reconfigure scheduling.

NOTE

Implicit rules

After migrating a configuration to version 9, implicit rules (*Security policy > Implicit rules* menu) will be enabled, regardless of their status in version 8. If you have disabled these rules, you will need to check them again when checking the rest of your policy in version 9.

Typical order of a migrated policy

		FILTERING NAT							
		Searched text X + New rule - Delete Up Down Expand all Collapse all Cut Copy Paste							
		Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	Comment
A.	1	on	pass	host_bypass	Any	Any		Firewall	
B.	2	on	pass	Any	host_bypass	Any		Firewall	
C.	3	on	pass	Internet	firewall_all	firewall_srv https			Admin from everywhere
	4	on	pass	Any	firewall_all	Any	icmp (Echo request)		Allow Ping from everywhere
	5	on	pass	Any interface: in	Any	pop3		Mail filter: default00	pop3 proxy
	6	on	pass → HTTP proxy	Any interface: in	Firewall_out	http_proxy			
D.	7	on	pass	Any interface: in via Explicit HTTP proxy	Any	http		URL filter: default00	proxy explicite
	8	on	pass	Any interface: dmz3	Any	ftp		FTP Filtering	ftp proxy
	9	on	pass	Any interface: dmz2	Any	smtp		Mail filter: default00	smtp proxy
E.	10	on	block	Any	Any	Any			Block all
F.	V8 policies migrated								
	11	on	pass	Any	Any	Any			
	12	off	block	host_1	host_2	Any			
	13	on	pass	host_1	host_2	Any			test
	14	on	pass	Any	Any	Any			
	15	on	pass	Any	Any	Any			
	16	on	pass	Any	Any	Any			
	17	on	pass	Any	Any	http	HTTP		
	18	on	pass	Any	Any	domain_udp	DNS/udp		
	19	on	pass	Any	Any	domain_udp	DNS/udp	DS	
G.	20	on	pass	Any	Any	domain_udp	udp		

A. Whitelist:

The configuration of a host *whitelist* (ASQ Bypass) in V8 has been migrated in the form of two filter rules for each V8 whitelist entry. Both rules, in Firewall mode, filter incoming and outgoing traffic respectively.

B. Accessing the Firewall:

A rule allows routing and authorizing access in HTTPS (443) and TCP_1300 from a remote management host. You can access the firewall via the web administration interface and through the firewall_srv service.

C. Ping:

A rule allows pinging the firewall.

D. Proxies:

In a V8 configuration, implicit rules generated when proxies are enabled on certain interfaces (General proxy configuration window) are rewritten according to each protocol and interface.

Access to the explicit HTTP proxy is allowed by two filter rules – one enables the proxy's service and the other allows traffic through this proxy (rules 6 & 7).

The URL and Mail filter policies have been reinitialized, and therefore need to be rewritten.

E. Blocking:

The “Block all” rule allows disabling the filter rules imported after it. This rule has to be deleted after the migrated rules have been modified.

F. Separator:

This separator with the title “migrated V8 policy” indicates that imported rules have been inserted under it.

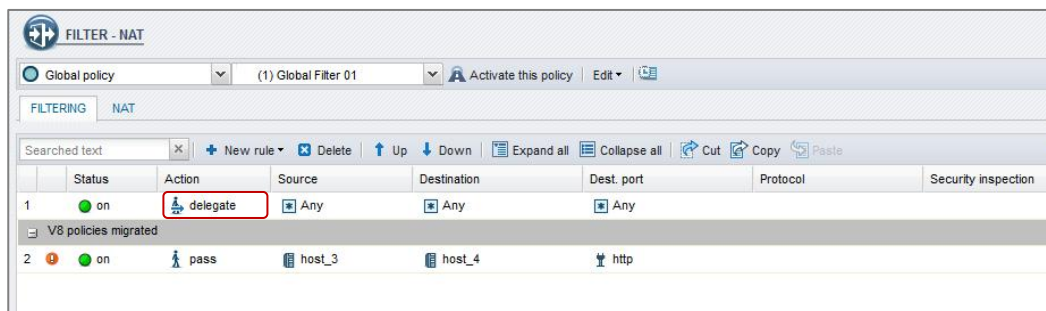
G. Migrated v8 filter rules:

The ON and OFF statuses have been retained but the active rules are not applied because of the previous “Block all” rule. These rules have to be validated manually.

Example of a migrated Global policy

To view the menu that allows displaying the Global policy in version 9, go to **Preferences**, which can be accessed by clicking on  in the banner at the top of the screen. Next, select the option *Display the global security policy (Filtering and NAT)*.

By default, the option **Delegate** – specific to global filter policy rules – makes it possible to assign priority to the local policy. Thanks to this rule, the application of these imported global rules can be delayed so that they can be modified. This rule can be deleted once the changes have been made.



Compatibility of V8 and V9 filter rules

Status	on	retained	
	off	retained	
Interface	auto	retained	
	others (in, out...)	retained	
DSCP service	All	retained	
Protocol	tcp	retained	
	udp	retained	
	icmp	retained	
	Others (egp, eigrp, ggp, gre...)	retained	
Message	All (network inaccessible, protocol inaccessible...)	retained	
Source	User	retained	
	Host	retained	
	Operators	retained	
Source port	Port	retained	
	Operators	retained	
Destination	Host	retained	
	Operators	retained	
Destination port	Port	retained	
	Operators	retained	
Action	none	retained	The action becomes "Log"
	Pass	retained	
	Block	retained	
	Reinitialize	retained	
	Count	retained	
	Rate	retained	
	DSCP rewrite	retained	
Routing		retained	
QoS		retained	
Logs	No log	retained	
	Log	retained	
	Minor	retained	
	Major	retained	
ASQ options	Profile	partially	ASQ profile reset to factory settings
	Do not attach plugins	partially	Rule in Firewall mode
	No contextual signatures	partially	Rule in IDS mode
Rule name		retained	
Description		retained	

Migrating the NAT policy

Main points

NAT rules have been correctly migrated, so no modifications are necessary in general. However, rules will need to be re-ordered because of the new rule assessment.

REMINDER

Migration retains only the **active slot** of the V8 configuration.

The **scheduling** feature will not be migrated. You will need to assign a time object in the *action* column of a rule in order to reconfigure scheduling.

Impact of destination NAT on filtering

In version 8, NAT on the destination is applied before filtering, and filtering is therefore applied on traffic with a translated destination.

Version 9 applies filtering before NAT, therefore traffic is filtered by its original destination. The destination object of a filter rule therefore has to be modified by indicating the original instead of the translated source.

Ordering of rules

In version 8, the most specific rules are assessed as a priority. From version 9 onwards, the execution of a rule cancels the execution of the rules that follow it – the order in which rules are assessed is therefore kept.

To ensure that the results of the assessment of a V8 policy migrated to V9 are correct, rules have to be re-ordered.

Example 1

A network *mynetwork* and a host *myhost*, with *myhost* belonging to *mynetwork*.

Rule1: *mynetwork* translated to IP address 1.1.1.1

Rule2: *myhost* translated to IP address 2.2.2.2

In V8, the IP address of a packet originating from *myhost* would correspond to rule 2, whereas in V9, it would correspond to rule 1.

Example 2

When we have the following in a NAT policy:

- **A rule that translates all traffic with the firewall's outgoing IP address,**
- **A bi-directional translation rule for a particular host.**

In version 8, the outgoing rule can be placed before the bi-directional rule.

In version 9, the order in which a rule appears in a policy prevails. It is therefore best to place particular translation rules first.

Differences between V8 and V9

In version 8, the actions "map", "nomap", "bimap", "rdr" and "split" clearly indicated the translation operation to be performed.

In version 9, translation operations are defined by the values assigned to the source and destination fields ("nat" action only).

WARNING

The translation of the source (Nat and Bimap) requires the definition of the interface in the Destination column in V9, whereas it was automatic in V8.

Exclusion rule for transparent proxies (HTTP, FTP, POP3 and SMTP)

The example of an exception for the transparent HTTP proxy, for HTTP traffic to an intranet, for example, could be configured by a redirection of a server to itself. This exception bypassed the translation operation by the assessment rule that gives priority to the most specific rules in version 8.

In version 9, these exceptions can be configured in the filter policy by adding a rule that authorizes specific traffic without being scanned.

Options

In version 9, dynamic connections needed for certain protocols (FTP/ RealAudio/ H323 (VOIP) / Netbios) are now automatically opened in V9.

Proxy options are therefore no longer necessary.

Map

This rule has been fully migrated and does not require modifications to filtering as translation is conducted at the source.

In version 8, the action **map** is used to translate a network with an internal address range using the firewall's public IP address to any (n for 1).

Status	Interface	Action	Option	Original Source	Destination	Destination Port	Translated	Translated Port	
1	On	out	map	Aucun	Client	<Any>	<Any>	Firewall out	ephemeral fw

In V9, 'any' can be replaced with 'Internet' (as opposed to 'Network_internals')

		Original traffic (before translation)				Traffic after translation			
	Status	Source	Destination	Dest. port		Source	Src. port	Destination	Dest. port
1	 on	 client	 Any interface: out	 Any		 Firewall_out	 ephemeral_fw	 Any	








Nomap

Like the previous rule, this rule has been fully migrated and does not require modifications to filtering as translation is conducted at the source.

A **nomap** rule allows traffic to keep the IP address of the original source. Packets from the source to the destination on the outgoing interface are therefore not translated and keep the same source IP address (n for n).

Status	Interface	Action	Option	Original Source	Destination	Destination Port	Translated	Translated Port
1	out	no map	none	client	<Any>	<Any>	<Any>	<Any>

This rule is replaced during migration with a NAT rule that translates the source, which will no longer have *none* as the translated source, but the original source object.

Original traffic (before translation)					Traffic after translation				
	Status	Source	Destination	Dest. port		Source	Src. port	Destination	Dest. port
1	 on	 client	 Any interface: out	 Any		 client		 Any	

Bi-directional map (bimap)

In version 8, the **bi-directional map** feature is used for translating the private IP address of a host (or of a network) to a public IP address (or a public network). This translation (1 for 1) has to operate in both directions (incoming and outgoing).

V8 NAT and filter rules

Status	Interface	Action	Option	Original Source	Destination	Destination Port	Translated	Translated Port
1	out	bidirectional map	none	internal_server	<Any>	<Any>	virtual_server	<Any>

Status	Protocol	Source	Destination	Destination Port	Action
1	all	internal_server	<Any>	<Any>	pass
2	all	<Any>	internal_server	<Any>	pass














In version 9, this operation is represented by 2 rules – one performs translation on the incoming traffic, the other on outgoing traffic. This rule has been fully migrated but requires modifications to filtering as translation is applied on the destination.













REMINDER

In V9, filtering is performed **before** address translation – the migrated filter policy has to be modified in order to be based on the original IP addresses of the hosts selected in *Destination* ❶ and no longer the translated IP addresses.

V9 NAT and filter rules

Original traffic (before translation)					Traffic after translation				
	Status	Source	Destination	Dest. port		Source	Src. port	Destination	Dest. port
1	 on	 internal_server	 Any interface: out	 Any	➡	 virtual_server		 Any	
2	 on	 Any interface: out	  virtual_server	 Any	➡	 Any		 internal_server	

	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
1	 on	 pass	 internal_server	 Any	 Any		
2	 on	 pass	 Any interface: out	 virtual_server	 Any		

Redirection (rdr)

In V8, the Redirection rule allows translating a public IP address associated with a port to a private IP address on an identical or different port (1 for n or n for n).

Status	Interface	Action	Option	Original Source	Destination	Destination Port	Translated	Translated Port
1	On	out	redirect	none	<Any>	virtual_server	http	internal_server

This rule is also correctly migrated but filtering needs to be modified, as translation is applied to the destination.

REMINDER

In V9, filtering is performed **before** address translation – the migrated filter policy has to be modified in order to be based on the original IP addresses of the hosts selected in *Destination* ❶ and no longer the translated IP addresses.

Original traffic (before translation)					Traffic after translation			
	Status	Source	Destination	Dest. port	Source	Src. port	Destination	Dest. port
1	on	Any interface: out	virtual_server	http	Any		internal_server	http

NOTE

The alternative method that allows performing this redirection in V9 is to use the filter policy directly. Indeed, a redirection operation can be associated with the traffic's destination IP address.

In the **Destination** column, select an object in the section *NAT on destination* in the *Advanced properties* tab.

	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
1	on	pass	Any interface: out	virtual_server → internal_server	http		

Redirection with load balancing (split)

This rule is similar to a Redirection rule, with the additional function on the destination after translation – Load balancing using the round-robin method. This type of load balancing allows, for example, sending traffic to a series of servers that take turns.

Status	Interface	Action	Option	Original Source	Destination	Destination Port	Translated	Translated Port
1	On	out	split	none	<Any>	virtual_server	http	loadbalanced_servers

This rule has been fully migrated but filtering needs to be modified, as translation is applied to the destination.

REMINDER

In V9, filtering is performed **before** address translation – the migrated filter policy has to be modified in order to be based on the original IP addresses of the hosts selected in *Destination* ❶ and no longer the translated IP addresses.

Original traffic (before translation)					Traffic after translation			
	Status	Source	Destination	Dest. port	Source	Src. port	Destination	Dest. port
1	on	Any interface: out	virtual_server	http	Any		loadbalanced_servers	

NAT on non-TCP/UDP/ICMP protocols (Example: GRE)

V8 rules allowed translating these protocols by managing sessions (stateful). However, as filtering did not handle these protocols with this level of status tracking, two rules were therefore needed to authorize incoming and outgoing traffic.

In V9, the rules do not track statuses by default for these protocols. This setting is different in V9 as it is now carried out in the filter policy. As a result, NAT rules are migrated but are not operational.

To make the translation operation effective, filter rules that allow traffic on these protocols have to be modified by selecting the required type of IP protocol in the *Protocols* column and by selecting the option “Status tracking (stateful)”.

Take the case of PPTP









PPTP is a PPP over IP encapsulation protocol that uses a control channel via a TCP session on port 1723 and a data channel by using the GRE IP protocol. The translated GRE packet will be translated but not its response. The option therefore needs to be added in the associated filter rule.











V8 NAT and filter rules

Status	Interface	Action	Option	Original Source	Destination	Destination Port	Translated	Translated Port	Description
1	On	out	map	none	client	<Any>	<Any>	Firewall_out	ephemeral_fw

Status	Interface	DSCP	Service	Protocol	Message	Source	Source Port	Destination	Destination Port	Action
1	On	auto		gre		client	<Any>	server	<Any>	pass
2	On	auto		gre		server	<Any>	client	<Any>	pass

Rules migrated in V9

Original traffic (before translation)					Traffic after translation				
	Status	Source	Destination	Dest. port		Source	Src. port	Destination	Dest. port
1	 on	 client	 Any interface: out	 Any		 Firewall_out	 ephemeral_fw	 Any	

	Status	Action	Source	Destination	Dest. port	Protocol
1	 on	 pass	 client	 server	 Any	gre
2	 on	 pass	 server	 client	 Any	gre

If NAT rules allowed reaching a PPTP server in V8, the GRE protocol is no longer translated statefully after an upgrade to V9. It is therefore necessary to correct the filter rule in which the client initiates the connection by enabling the *stateful* option (*Protocol* column), and then delete the second rule.

Corrected filter rule

	Status	Action	Source	Destination	Dest. port	Protocol
1	on	pass	client	server	Any	gre

NAT option in the IPSec tunnel

This option, which is equivalent to 'Nat before VPN' in version 8, has been correctly migrated. Via this option, which is common to the whole NAT policy, the translation operation is executed before encryption and after decryption.

In V9, this option becomes more flexible as it can be applied rule by rule (*option* column).

End of the double assessment of the policy

In V8, assessments of the NAT policy are carried out in succession: one before filtering (incoming) for the translation of the destination and one after filtering (outgoing) for the translation of the source.

As a result, in order to modify both the source and destination of a connection, two rules were needed (*Redirect* and *Map* rules for example).

In V9, a single assessment of the NAT policy is done. If both the destination and the source need to be modified, only a single rule is needed.

During migration, all the rules in the NAT policy are migrated. If two rules modified the destination and the source, both rules will appear in V9 but only one rule can be applied. **The necessary changes therefore need to be made to one of the rules as a result, before deleting the second rule.**

Example

A first rule redirects traffic going towards `virtual_server` to a public IP address (`public_IP`). The second rule changes the source address to the address of the service provider for traffic to the internet.

V8 policy: a redirect and map rule are applied.

	Status	Interface	Action	Option	Original Source	Destination	Destination Port	Translated	Translated Port
1	On	out	redirect	none	<Any>	virtual_server	<Any>	internal_server	<Any>
2	On	dmz1	map	none	<Any>	internal_server	<Any>	Firewall_dmz1	ephemeral_fw

V9 policy: the source of traffic towards `virtual_server` will no longer be translated.

Original traffic (before translation)					Traffic after translation			
	Status	Source	Destination	Dest. port	Source	Src. port	Destination	Dest. port
1	on	Any interface: out	virtual_server	Any	Any		internal_server	
2	on	Any interface: dmz1	internal_server	Any	Firewall_dmz1		Any	

The simultaneous translation of the source and destination will no longer work. The user will need to modify his policy in order to add the second translation to the affected rules.

Corrected V9 policy:

Original traffic (before translation)					Traffic after translation			
	Status	Source	Destination	Dest. port	Source	Src. port	Destination	Dest. port
1	on	Any interface: out	virtual_server interface: dmz1	Any	Firewall_dmz1		internal_server	

Migrating the IPSec VPN policy

Local and Global IPSec VPN policies have been migrated.



REMINDER

Only the local policy will be available in the V9 web administration interface. The Global VPN policy can be accessed via the application NETASQ Centralized Manager.

The presentation of IPSec VPN policies changes in version 9. The module is organized around 4 configuration tabs:

Encryption policy - Tunnels

This window allows managing IPSec tunnels between two firewalls (*Site to site - Gateway-Gateway*) or between a NETASQ multifunction firewall and a mobile user (*Anonymous – Mobile users*).

Peers

Peer management (remote site or mobile anonymous peer) sets out in detail the parameters of the IKE profile, their negotiation method as well as the parameters specific to each negotiation method.

Identification

This tab allows listing the certificate authorities accepted in tunnels that use PKI methods as well as the pre-shared keys (PSK) in your mobile tunnels.

Encryption profiles

IKE (phase 1) and IPsec (phase 2) encryption profiles are listed in this section and allow establishing their maximum lifetime (in seconds). Negotiation proposals can also be defined at the same time as authentication and encryption algorithms.

Mobile users

User pre-shared keys saved in a local file on the firewall have been retained in version 9. As a general rule, they appear in the *Identification* tab. If a peer's ID is the same as its IP address, they will appear in the *Peer* tab.

In version 8, the pre-shared key can be defined in the peer's profile.

Information on pre-shared keys stored in the user's profile will not be retained during the migration of an internal user database (LDAP), due to the incompatibility of the formats of the internal database in both versions.

You are advised to use the **x-auth** authentication method, so that users will not need to enter a new password. This method uses the password entered in the user database (LDAP). However, this authentication method involves changing the VPN client's configuration.

Migrating the PKI

External public key infrastructures (PKI) can be migrated by upgrading the firmware or by restoring a configuration backup.



REMINDER

The partial migration of an internal LDAP database can only be carried out during the upgrade of the firewall from version 8 to version 9. The internal LDAP directory cannot be restored from a configuration backup file.

Data that will not be migrated are all NETASQ fields, including user pre-shared key data.