Stonesoft Corporation
Stonesoft Firewall and VPN

RSA SecurID Ready Implementation Guide

Last Modified: January 7, 2014

Partner Information

Product Information	
Partner Name	Stonesoft Corporation
Web Site	www.stonesoft.com
Product Name	Stonesoft Firewall and VPN
Version & Platform	5.4.3
Product Description	Stonesoft Security Platform unifies firewall, VPN and IPS, blending network security, end-to-end availability and award-winning load balancing into a unified and centrally managed system for distributed enterprises.

Solution Summary

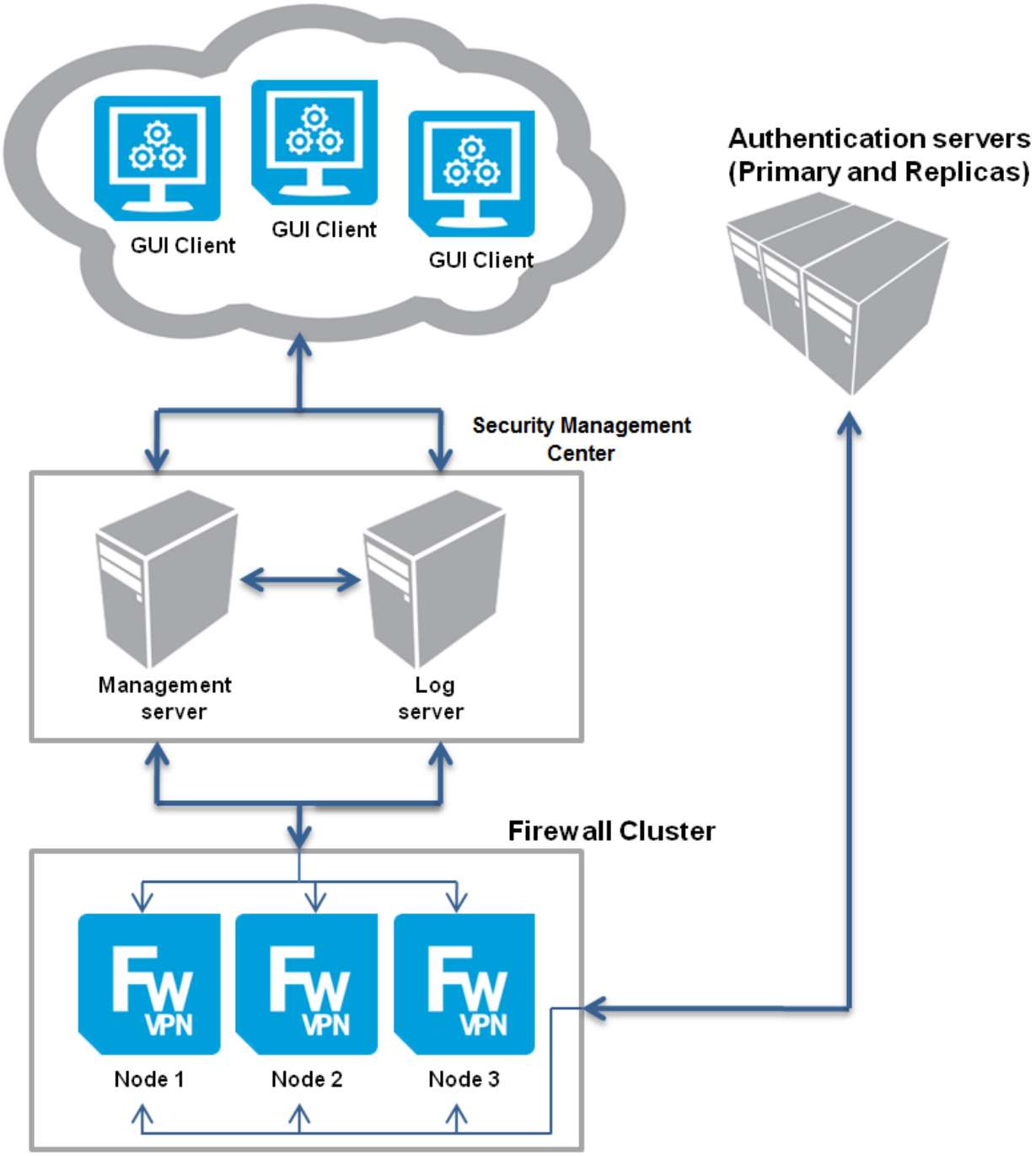
Stonesoft High Availability Firewall/VPN is a state-of-the-art firewall and Virtual Private networking (VPN) solution with built-in high availability features. Stonesoft combines the best traits of several firewall techniques to provide excellent security, performance and robustness. Stonesoft's clustering features eliminate the firewall as a potential single point-of-failure. Moreover, with Stonesoft's patented Multi-link technology, high availability can also be extended to network connections.

RADIUS is a back-end protocol used by Stonesoft to communicate with external authentication servers. RADIUS can be used together with RSA Authentication Manager to provide Stonesoft users secure two-factor authentication.

In external RADIUS authentication, the firewall engine queries an LDAP directory (either the Stonesoft's internal user database or an external server) for user identification data and the required authentication method. After receiving a response from the LDAP server regarding the user's method of authentication, the firewall sends an authentication request to the specified authentication service.

RSA Authentication Manager supported features	
Stonesoft Firewall and VPN 5.4.3	
RSA SecurID Authentication via Native RSA SecurID Protocol	No
RSA SecurID Authentication via RADIUS Protocol	Yes
On-Demand Authentication via Native SecurID Protocol	No
On-Demand Authentication via RADIUS Protocol	Yes
Risk-Based Authentication	No
Risk-Based Authentication with Single Sign-On	No
RSA Authentication Manager Replica Support	No
Secondary RADIUS Server Support	Yes
RSA SecurID Software Token Automation	No
RSA SecurID SD800 Token Automation	No
RSA SecurID Protection of Administrative Interface	No

Stonesoft System Architecture



Authentication Agent Configuration

Authentication Agents are records in the RSA Authentication Manager database that contain information about the systems for which RSA SecurID authentication is provided. All RSA SecurID-enabled systems require corresponding Authentication Agents. Authentication Agents are managed using the RSA Security Console.

The following information is required to create an Authentication Agent:

- Hostname
- IP Addresses for network interfaces

Set the Agent Type to “Standard Agent” when adding the Authentication Agent. This setting is used by the RSA Authentication Manager to determine how communication with Stonesoft Firewall/VPN engine will occur.

A RADIUS client that corresponds to the Authentication Agent must be created in the RSA Authentication Manager in order for Stonesoft Firewall/VPN engine to communicate with RSA Authentication Manager. RADIUS clients are managed using the RSA Security Console.

The following information is required to create a RADIUS client:

- Hostname
- IP Addresses for network interfaces
- RADIUS Secret

Note: Hostnames within the RSA Authentication Manager / RSA SecurID Appliance must resolve to valid IP addresses on the local network.

Please refer to the appropriate RSA documentation for additional information about creating, modifying and managing Authentication Agents and RADIUS clients.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Stonesoft Firewall/VPN engine with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

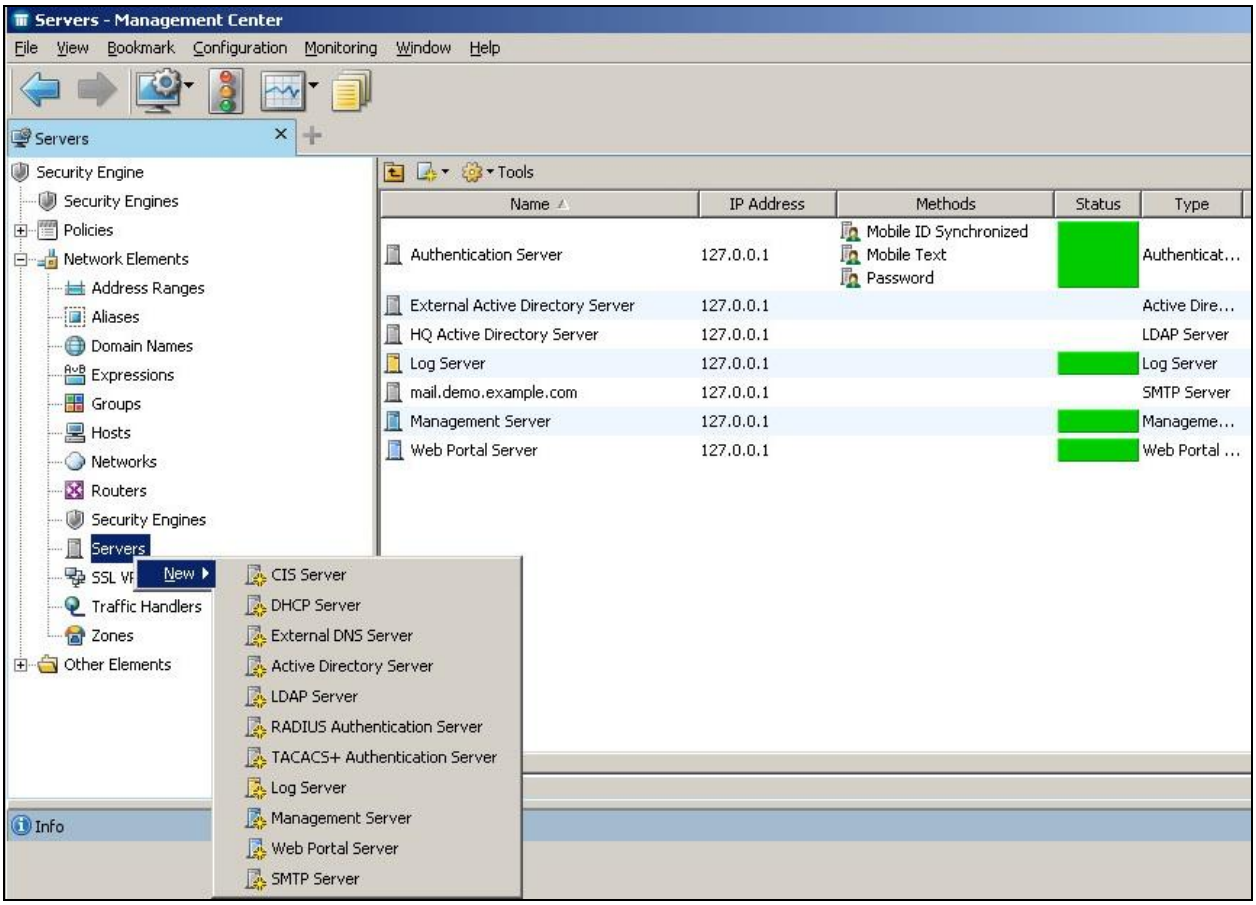
All Stonesoft Firewall/VPN engine components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Configuration Overview

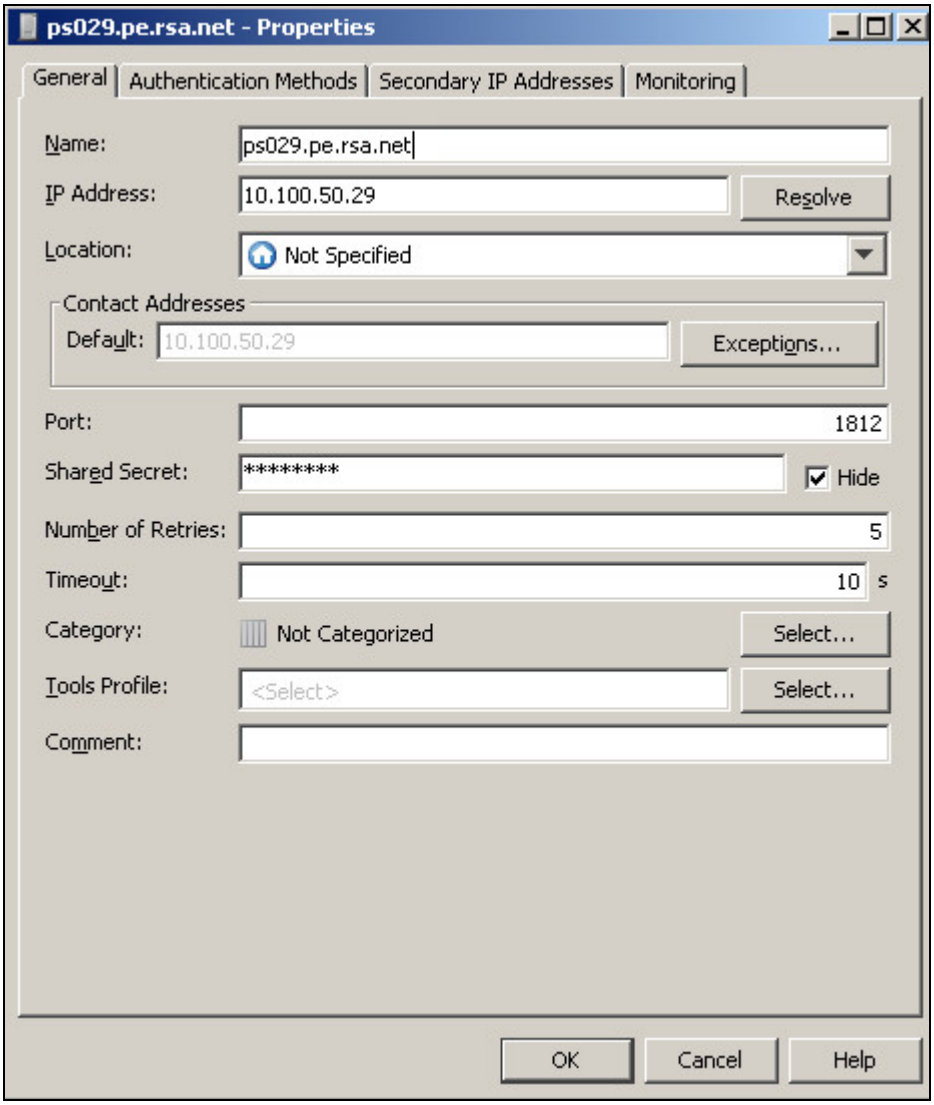
- Follow the steps outline in Stonesoft's documentation on configuring a **Basic VPN for Remote Clients**.
- Defining RADIUS Authentication Server.
- Defining Authentication Service.
- Defining users.
- Defining access rules.

Stonesoft Firewall/VPN RSA SecurID Authentication Configuration

1. Login to the Security Management Center (SMC).
2. From the top menu navigate to **Configuration > Configuration > Security Engine**.
3. From the left menu navigate to **Network Elements > Servers > New > RADIUS Authentication Server**.

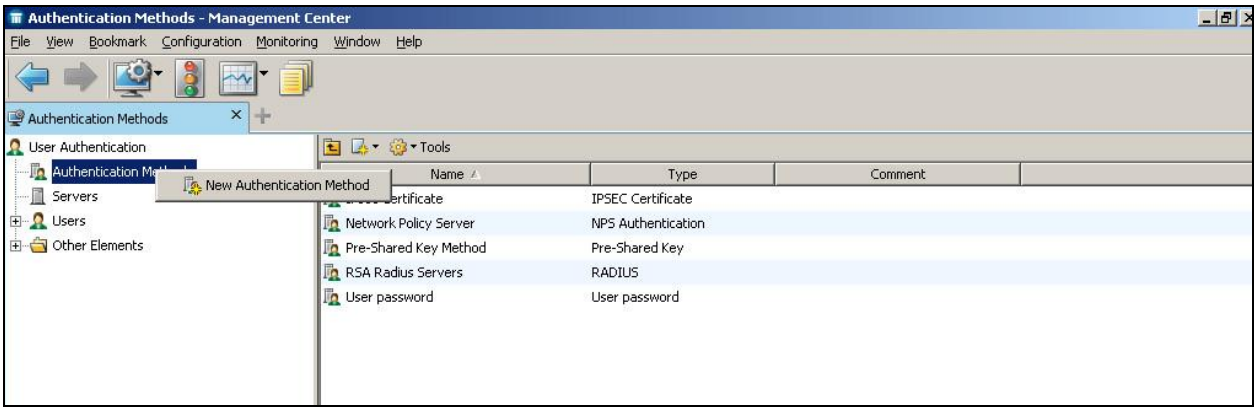


4. Configure the RADIUS Server fields for **Name, IP Address, Port Number**, and **Shared Secret**. Other fields may need to be modifed to match your environment.

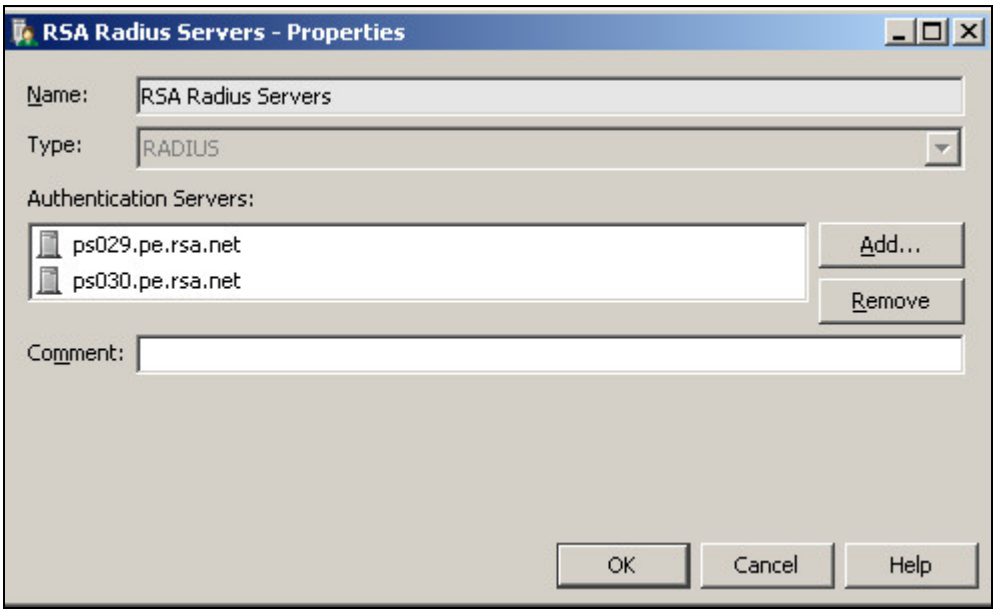


5. Click **OK**.
6. Repeat step 3 to add any secondary RADIUS servers.

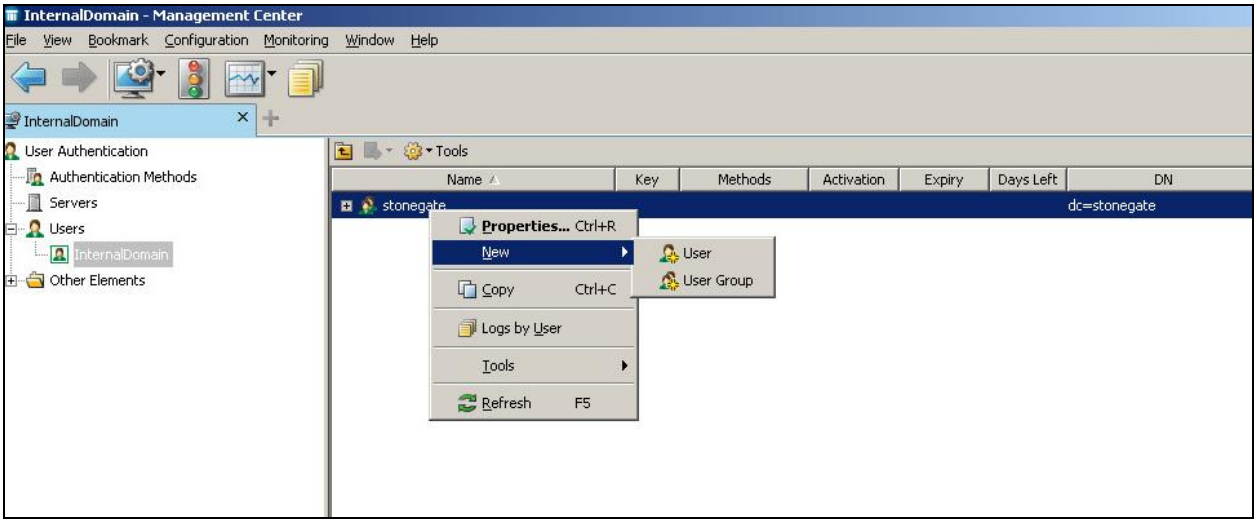
7. Create an Authentication Service which binds the RADIUS primary and secondary servers to the same service. Select **Configuration > Configuration > User Authentication**.
8. Right click **Authentication Methods** and select **New Authentication Method**.



9. Enter the **Name** and select the authentication type **RADIUS**.
10. Click **Add** and select the RADIUS servers.
11. Click **OK**.

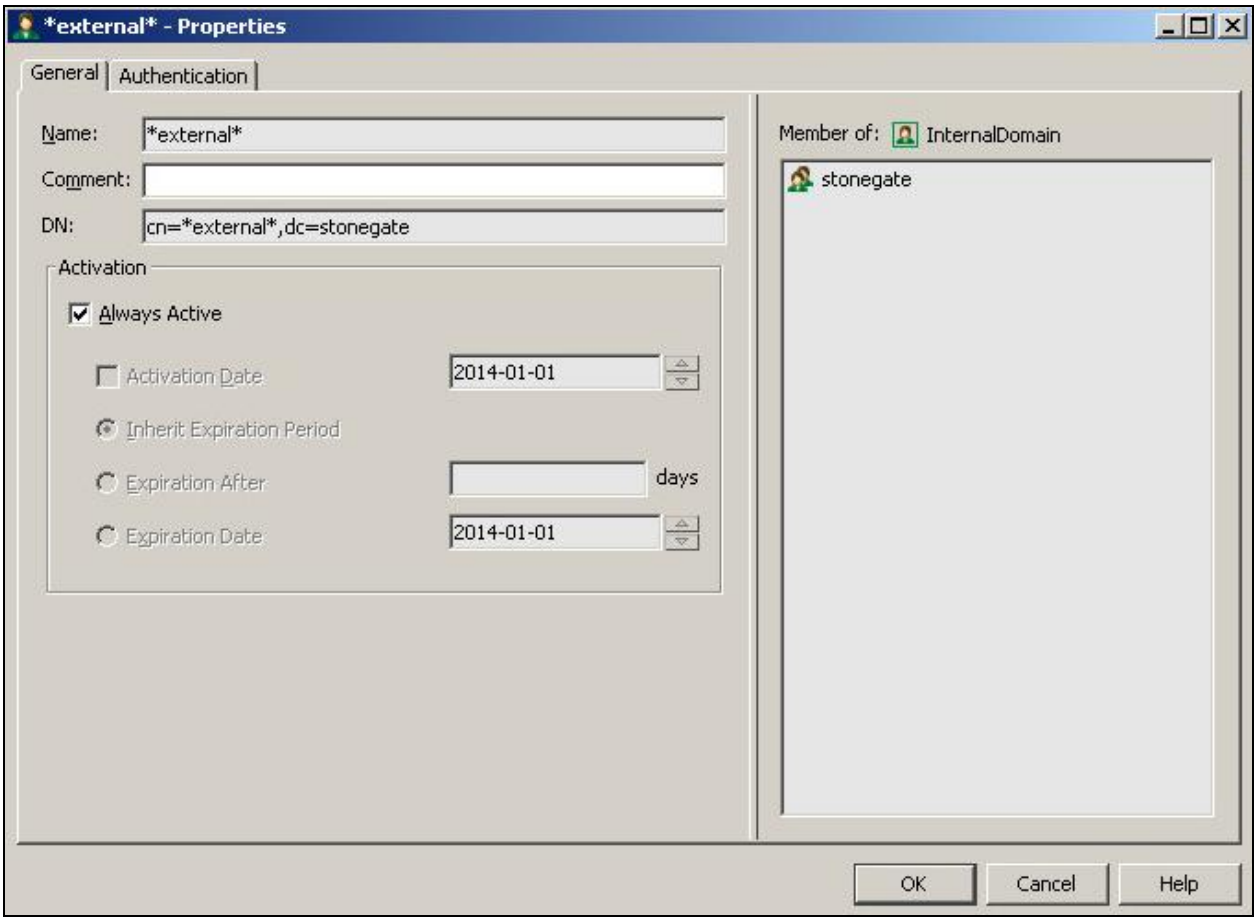


12. Create a User (or User Group) by navigating to **User Authentication > Users > InternalDomain** right click on **stonegate** and select **New > User**.

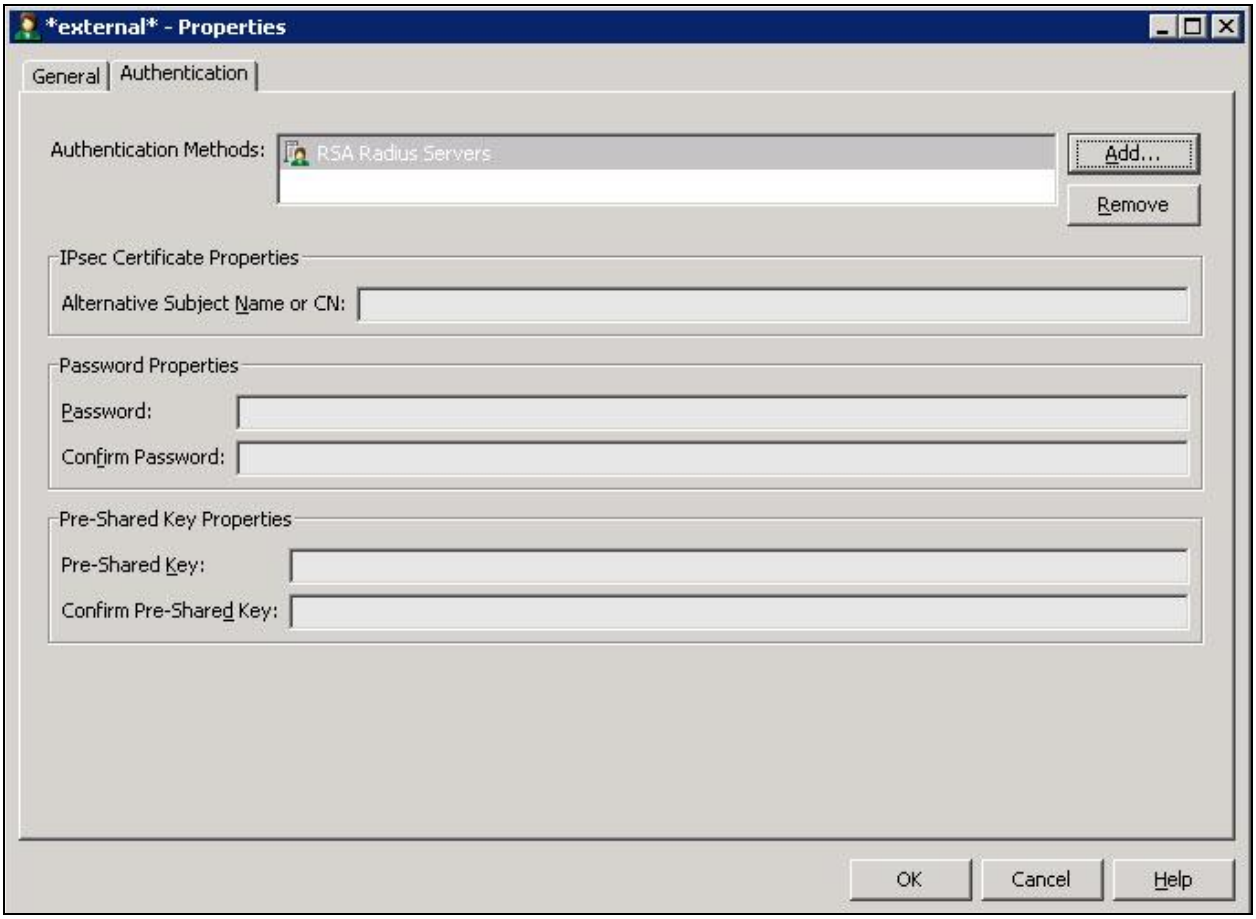


13. To configure RSA Authentication Manager as your default Authentication Service for all users, create a special user with the Name: ***external*** within the StoneGate User Database and bind it to the previously created Authentication Service. Using this generic method of authentication, ***external*** is the only user you will be required to create within the Stonesoft user database.

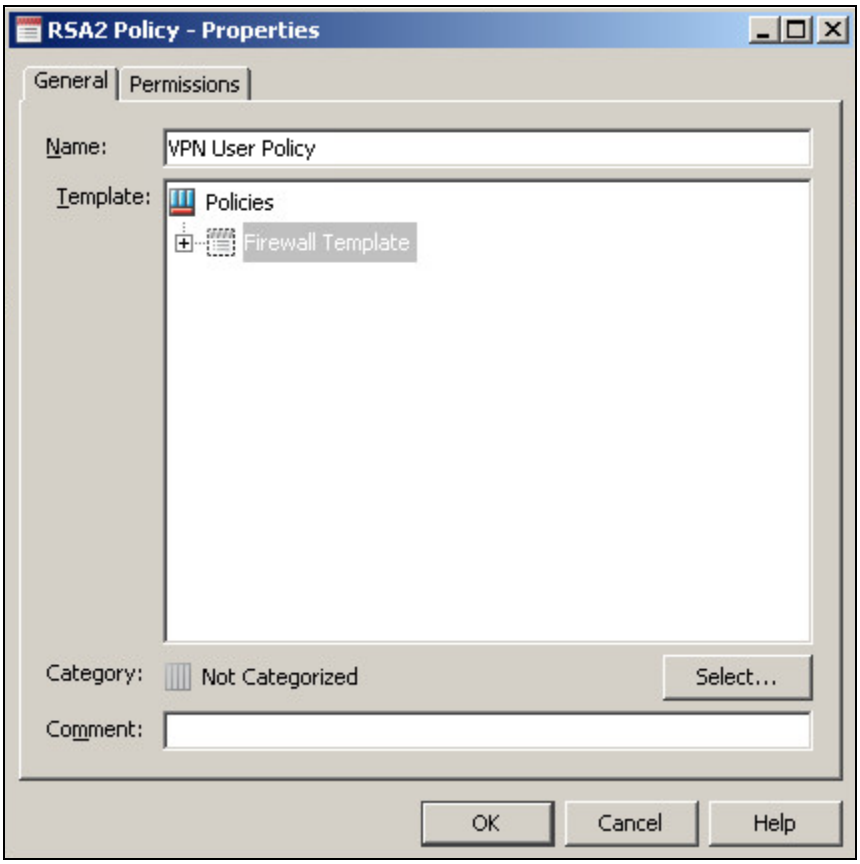
> **Note: If there is a need to configure Authentication Services on a per user basis, it can be done by creating individual user records within the Stonesoft User Database and binding them to the appropriate Authentication Service.**



14. Select the **Authentication** tab and click **Add.** Select the RADIUS Authentication Service you defined previously.

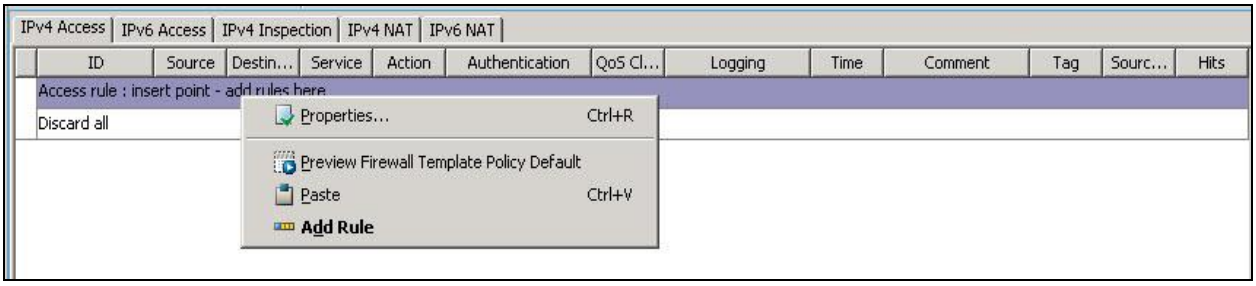


15. Select **Configuration > Configuration > Security Engine** from the top menu.
16. Expand **Policy** on the left menu.
17. Right-click the **Firewall Policies** branch.
18. Select **New > Firewall Policy.** The Firewall Policy Properties window opens.
19. Give the policy a **Name**.

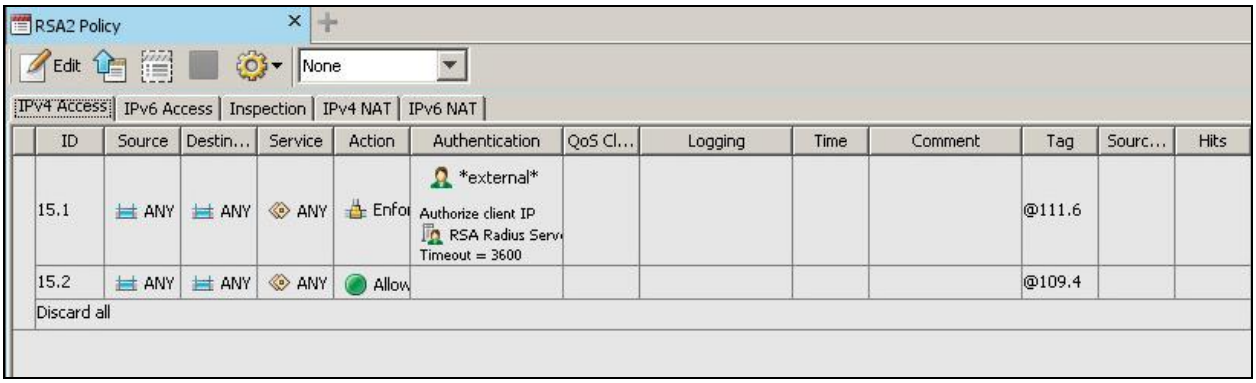


20. Select the **Template** you want to base this template or policy on.
21. Click **OK**. The new Template Policy or Policy opens in the Policy Editing view.

22. Right click **Access rule** and select **Add Rule**.

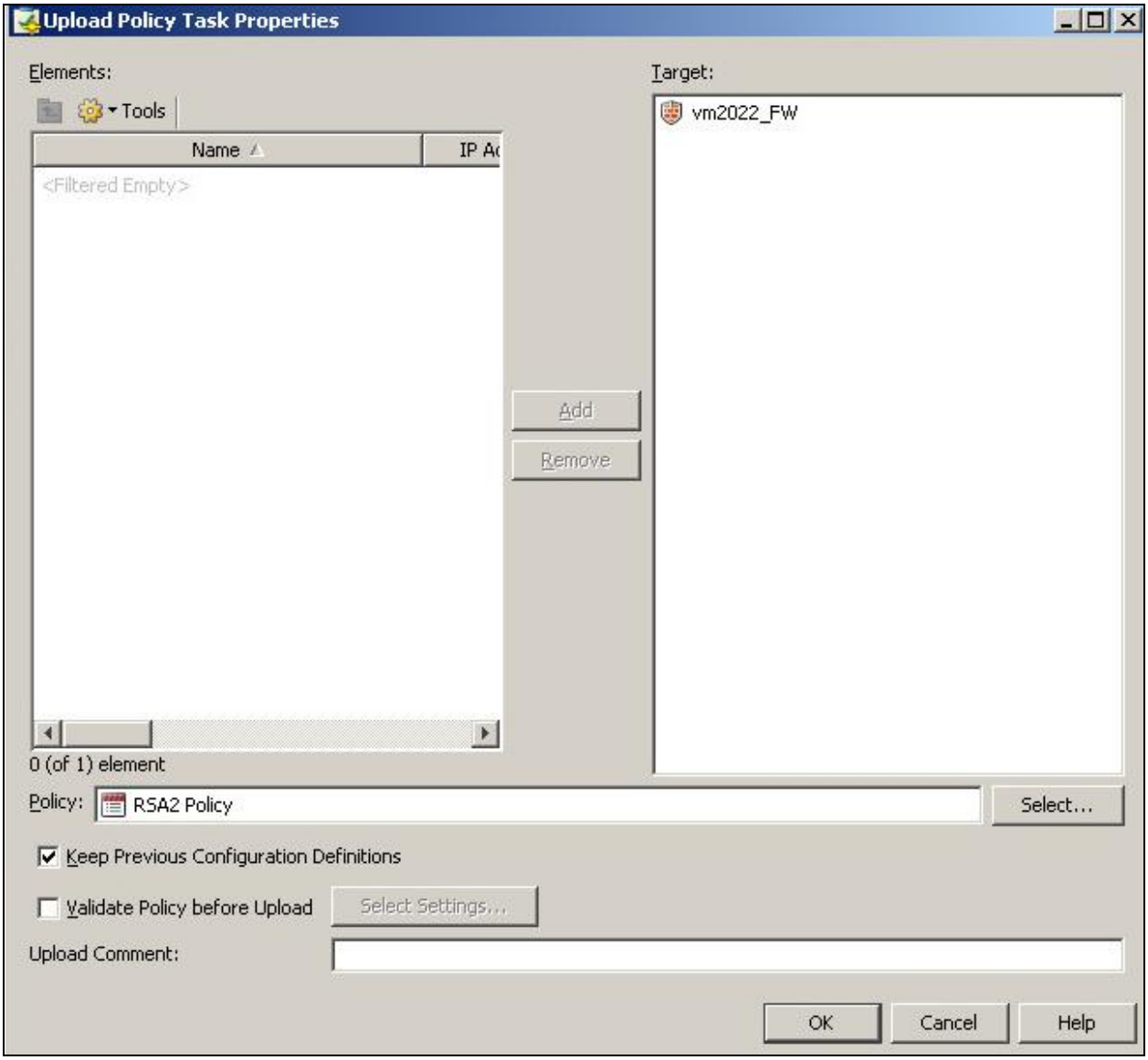


23. Right click in each field to define the desired policy rule.



24. Install the policy on the firewall to activate the configuration. Click the icon which looks like a notepad with a blue arrow pointing up.

25. The **Upload Policy Task Properties** window will open. Select the target Firewalls and click **OK.**



Note: For further details refer to Stonesoft's documentation.

RSA SecurID Login Screens

Login screen:

User-defined New PIN:

System-generated New PIN:

Next Tokencode:

Certification Checklist for RSA Authentication Manager

Date Tested: January 7, 2014

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	8.0	Virtual Appliance
Stonesoft Management Client	5.5.4	Windows 2008 Server R2
Stonesoft Firewall and VPN	5.4.3	Stonesoft Linux
Stonesoft IPsec VPN Client	5.4.1	Windows XP

Mandatory Functionality			
RSA Native Protocol		**RADIUS Protocol**	
New PIN Mode			
Force Authentication After New PIN	N/A	Force Authentication After New PIN	✓
System Generated PIN	N/A	System Generated PIN	✓
User Defined (4-8 Alphanumeric)	N/A	User Defined (4-8 Alphanumeric)	✓
User Defined (5-7 Numeric)	N/A	User Defined (5-7 Numeric)	✓
Deny 4 and 8 Digit PIN	N/A	Deny 4 and 8 Digit PIN	✓
Deny Alphanumeric PIN	N/A	Deny Alphanumeric PIN	✓
Deny PIN Reuse	N/A	Deny PIN Reuse	✓
Passcode			
16-Digit Passcode	N/A	16-Digit Passcode	✓
4-Digit Fixed Passcode	N/A	4-Digit Fixed Passcode	✓
Next Tokencode Mode			
Next Tokencode Mode	N/A	Next Tokencode Mode	✓
On-Demand Authentication			
On-Demand Authentication	N/A	On-Demand Authentication	✓
On-Demand New PIN	N/A	On-Demand New PIN	✓
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	N/A	Failover	✓
No RSA Authentication Manager	N/A	No RSA Authentication Manager	✓

GLS

✓ = Pass ✗ = Fail N/A = Not Applicable to Integration