Fortinet
FortiGate

RSA SecurID Ready Implementation Guide

Last Modified: April 15, 2011

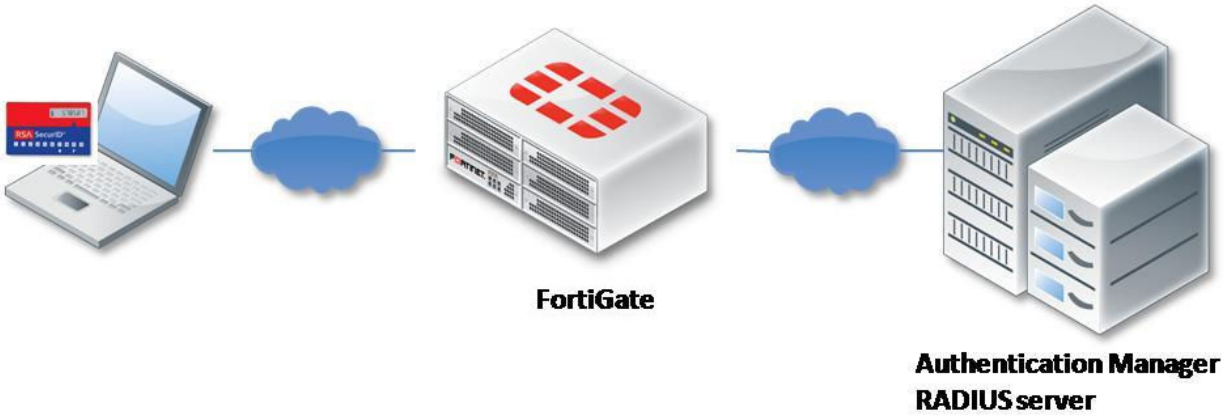
Partner Information

Product Information	
Partner Name	Fortinet
Web Site	www.fortinet.com
Product Name	FortiGate
Version & Platform	3950B – v4.3.0
Product Description	The FortiGate-3950 series of consolidated security appliances offers unmatched performance, flexibility, and security for large enterprise networks and service providers. FortiGate-3950B and FortiGate-3951B appliances combine high-performance hardware and a modular design to deliver the fastest firewall throughput available in any appliance form factor. They also protect your network with Fortinet's unmatched depth and breadth of security services.

Solution Summary

For Fortinet RSA integration was decided to use the RSA Secured Partner Certification Portal because it provides an instance of the Authentication Manager together with the RADIUS server.

In the following figure there is the diagram of the test environment:



There are several possibility to trigger authentication mechanism on Fortinet product:

- L2TP
- PPTP
- Firewall authentication
- Wireless authentication
- Administrator authentication
- IPsec
- SSL-VPN

In this test scenario, to easy the tests, was used the identity based policy in the firewall policy. Fortinet products support a Primary and a Secondary instance of the RADIUS server. There are four kinds of authentication scheme supported: MS-CHAP-v2, MS-CHAP, CHAP, PAP.

RSA SecurID supported features	
FortiGate-3950	
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
On-Demand Authentication via API	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

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 FortiGate-3950 will occur.

A RADIUS client that corresponds to the Authentication Agent must be created in the RSA Authentication Manager in order for FortiGate-3950 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 FortiGate 3950B with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

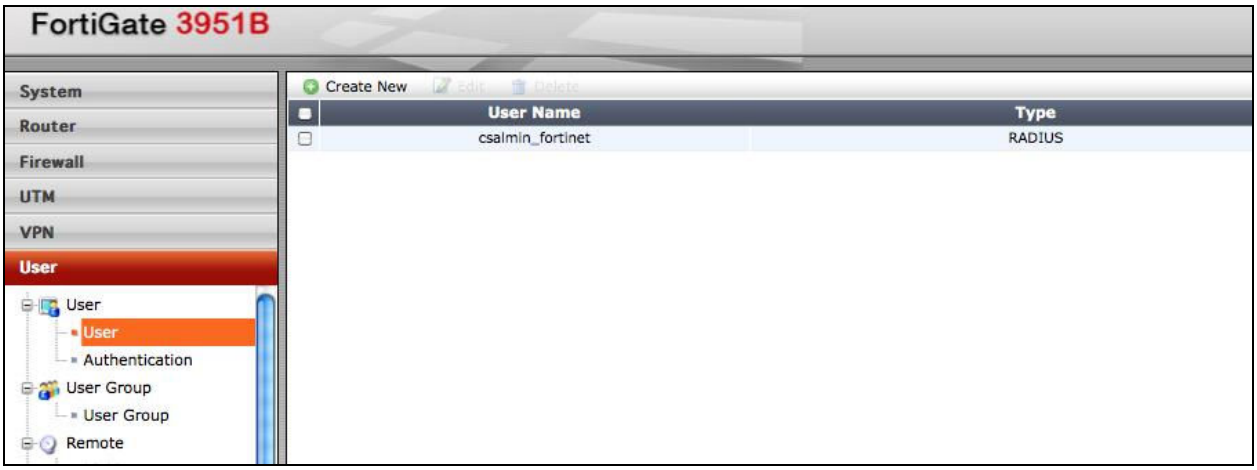
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All FortiGate 3950B components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

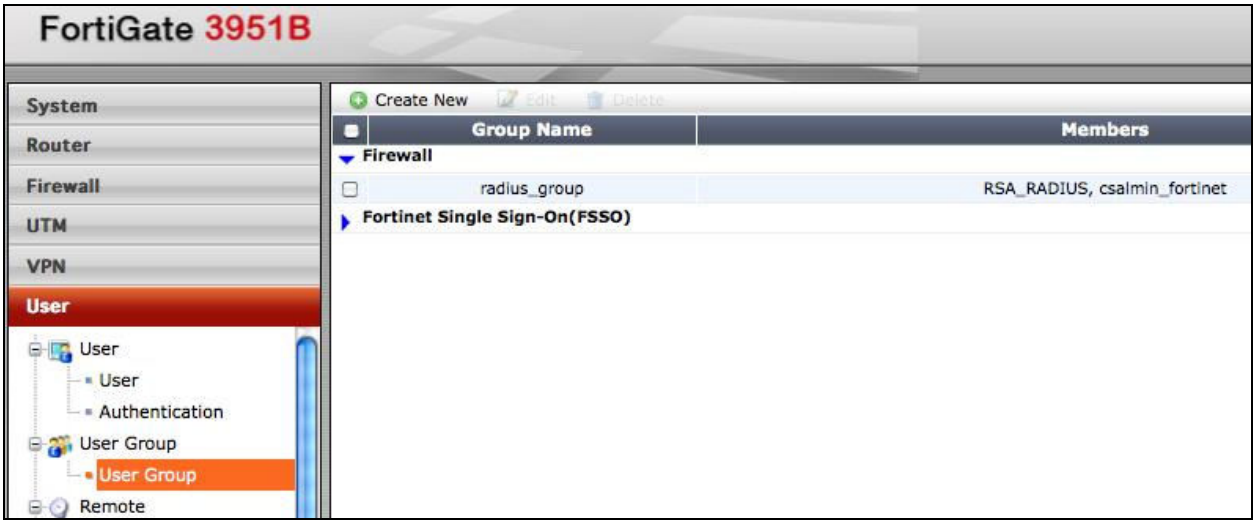
Documenting the Solution

In order to configure the FortiGate 3950B the following steps must be followed:

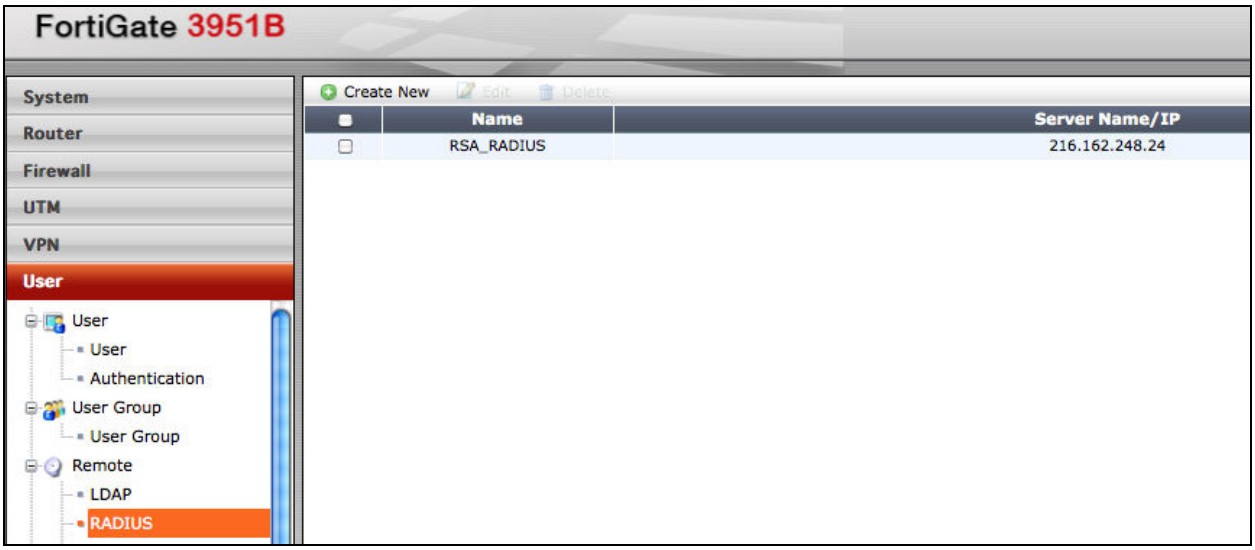
1. Add user(s).



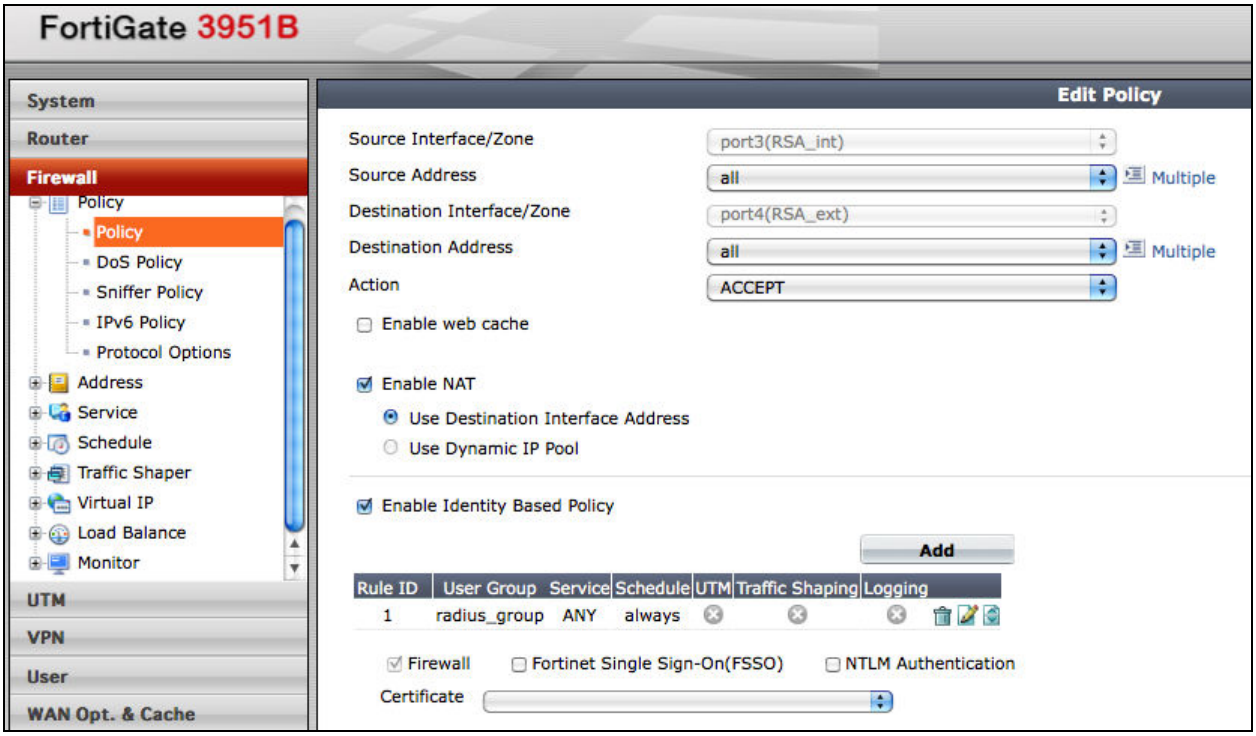
2. Add user group(s) which includes all the users you want to authenticate.



3. Add a RADIUS server.

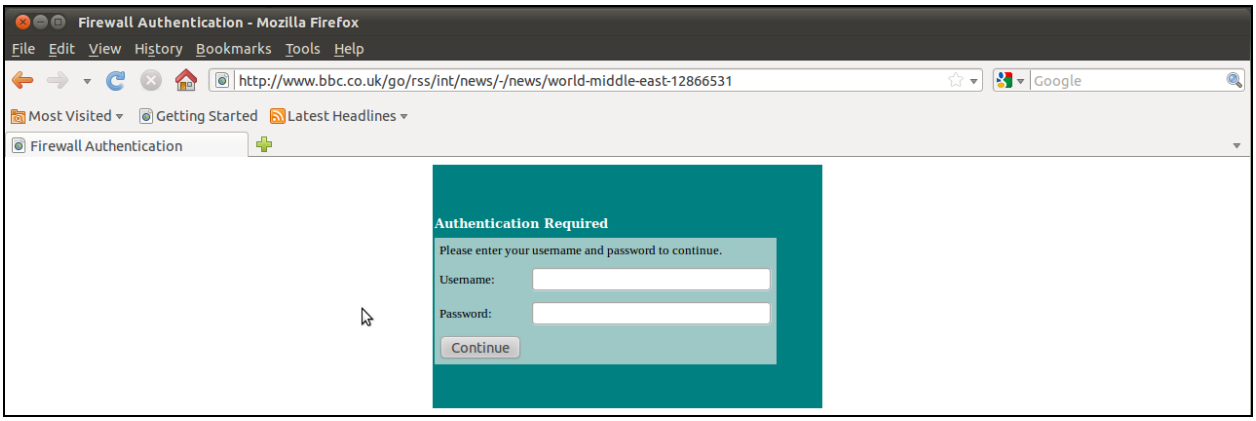


4. Create the firewall policy and enable the “Identity Based Policy” and add the group(s) you want to authenticate against this policy.

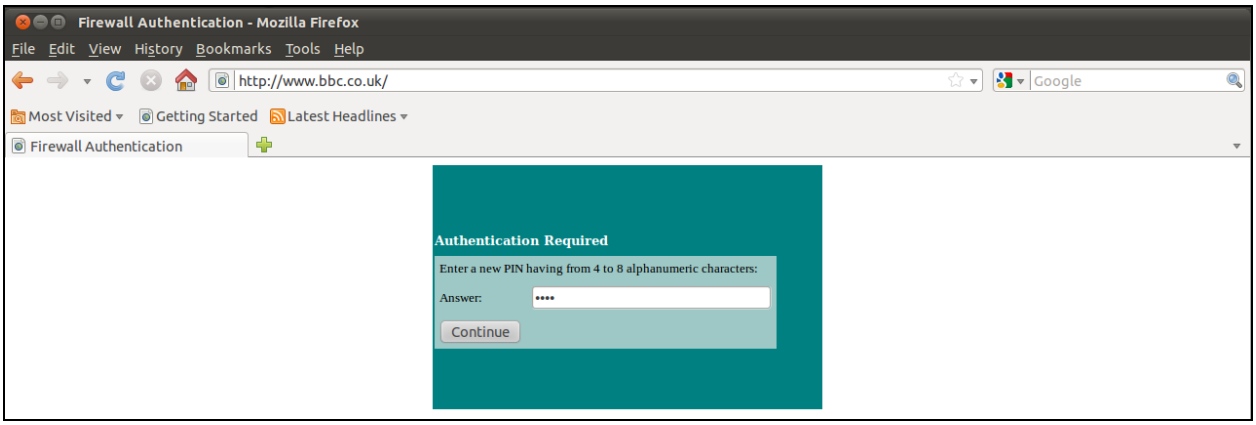


Screens

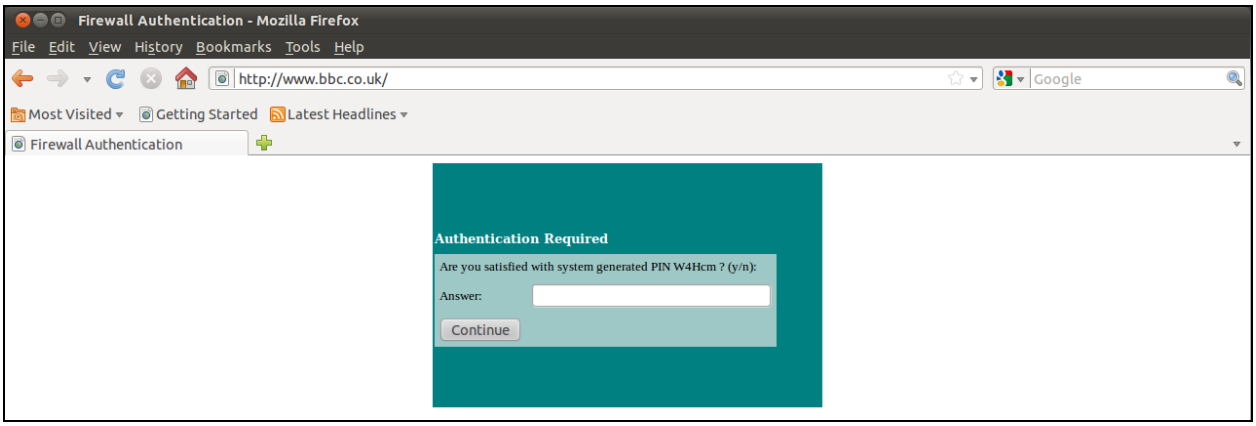
Login screen:



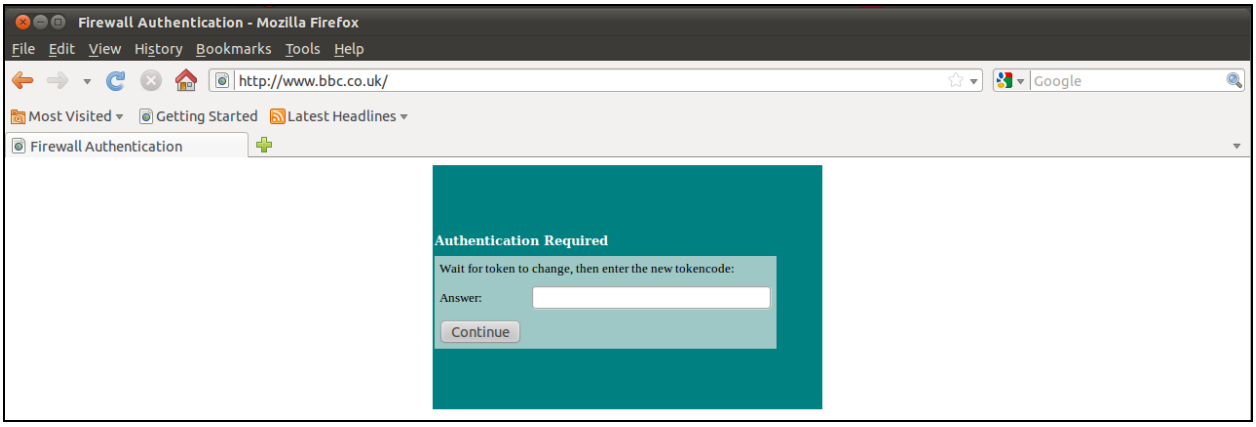
User-generated New PIN:



System-generated New PIN:



Next Tokencode:



Certification Checklist for RSA Authentication Manager

Date Tested: April 5, 2011

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	7.1 SP4	Windows 2003 SP4
FortiGate	3950B – v4.3.0	Proprietary

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 Numeric PIN	N/A	Deny Numeric 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	✓

DRP / PAR

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