AppGate Security Server

Contents

- 1 Introduction
- 2 Prerequisites 2.1 Login Page customisation prerequisites
- 3 Baseline
- 4 Architecture
- 5 Swivel Configuration

 - ♦ 5.1 Configuring the RADIUS server
 ♦ 5.1.1 Enabling Session creation with username
 - ♦ 5.2 Setting up Swivel Dual Channel Transports
- - 6.2 Test the RADIUS authentication
 - 6.3 Optional: Login Page Customisation
- 7 Testing
- 8 Additional Configuration Options
- 9 Troubleshooting
- 10 Known Issues and Limitations
- 11 Additional Information

Introduction

This document describes steps to configure a AppGate Security Server from Cryptozone with Swivel as the authentication server. Swivel can provide Two Factor authentication with SMS, Token, Mobile Phone Client and strong Single Channel Authentication TURing, Pinpad or in the Taskbar using RADIUS.

Swivel integration is made using RADIUS authentication protocol with an option to configure the login page.

Prerequisites

AppGate Security Server Appliance

AppGate documentation

Swivel 3.x, 3.5 or higher for RADIUS groups

NAT for Single channel access

Login Page customisation prerequisites

Swivel server must be accessible by client when using Single Channel Images, such as the Turing Image, and security string number, for external access this is usually through a NAT.

Baseline

AppGate Security Server Appliance

Swivel 3.8

Architecture

The AppGate Security Server makes authentication requests against the Swivel server by RADIUS.

The client makes TURing requests against the Swivel server using HTTP/HTTPS

Swivel Configuration

Configuring the RADIUS server

On the Swivel Administration console configure the RADIUS Server and NAS, see RADIUS Configuration

Enabling Session creation with username

To allow the TURing image, Pinpad and other single channel images, under Server/Single Channel set Allow session request by username to Yes.

Setting up Swivel Dual Channel Transports

Used for SMS, see Transport Configuration

AppGate Security Server Configuration

Adding a Swivel RADIUS server

On the AppGate Security Server select Administration/Authentication Methods then Add Authentication Method.

Console Help			
	PinSafe (Radius)		
T appgate	Identifier radius/9		
Administration	Server configuration		
Authentication Methods Second Seco	Hostname(s)	swivel	
One Time Password (OTP) OTP+Password	Port(s)	1812	(Common ports
Radius	Retries	3	
RinSafe PinSafe+Password	Timeout(s)	7	(seconds)
▼ 👚 User Accounts 合 LDAP/AD	Shared secret	*****	
Cocal Accounts	Repeat shared secret	****	
 Access Rules Roles 	Use password for SSO		
 Unused Objects Satellites Logs Monitor and Status Clients 	Pick password from log Pick password from reg Add	gin dialog oly to any of these prompts: Delete	
 Run Commands System Settings 	Prompts		
	Initial prompt		
	Compatibility		
	Reject means reset (complies with RFC 5080 section 2.6.1)		
	Help		

It is recommended to use a password in combination with the OTC and this can be done by using a chained password.

Console Help	
	PinSafe+Password (Chained)
Administration Administration Authentication Methods Password One Time Password (OTP) OTP+Password OTP+Password Radius PinSafe PinSafe DAP/AD Cocal Accounts	PinSafe+Password (Chained) Identifier chained/10 Included methods Password PinSafe Add
System Settings	Help

On the AppGate Security Server select Administration/System Settings/SSL Access then select the required Authentication Methods allowed.

Console Help			
	SSL ACCESS		
	Certificate		
Authentication Methods			
Oser Accounts	Expires 2014-06-19 Host names appgate		
Access Rules			
Roles			
Unused Objects	Generate Upload Remove		
Satellites			
► 🔍 Logs	C		
Monitor and Status	Settings		
🔻 🔂 Clients			
Client Configuration Files	Listen on interfaces	✓ appgate	
🔕 Device Firewall rules			
🖏 Run Commands	Listen port	443	
🔻 🚜 System Settings			
🗢 AppGate Firewall rules	Title	SSL	
🐼 Backup & Restore			
A Built-in web server	DNS lookup timeout	10 Seconds	
The Connection Settings			
🚜 Daemons	Refresh time	5 Minutes	
💎 File System Manager			
File Transfer	Inactivity timeout	1 Hours	
L2TP/IPsec Access			
🔒 License Management	Cookie timeout	365 Days	
📥 Local Print	SSL Protocols	SSL 2.0 🗸 SSL 3.0 🗸 TLS 1.0	
🔍 Log settings	SSE FIOLOCOIS	□ 33L 2.0 V 33L 3.0 V 1L3 1.0	
Network/Cluster Management	SSL Protocol options	🗹 Allow MD5 hash	
🥖 Server Files	Authentication methods	Password 🗌 One Time Password (OTF	
Software Update	Admentication methods		
🔄 SSL Access			
Time Synchronization	Help		

Test the RADIUS authentication

At this stage it should be possible to authenticate by SMS, hardware Token, Mobile Phone Client and Taskbar to verify that the RADIUS authentication is working for users. Browse to the SSL VPN login page, and enter Username and if being used, the password. From the Swivel Administration console select User Administration and the required user then View Strings, and select an appropriate authentication string or OTC for the user. At the SSL VPN login enter the required OTC. Check the Swivel logs for a RADIUS success or rejected message. If no RADIUS message is seen, check that the Swivel RADIUS server is started and that the correct ports are being used.

Optional: Login Page Customisation

On the AppGate Security Server select Administration/User Accounts and for the required access account type ensure that RADIUS authentication is selecetd under the Authentication tab.

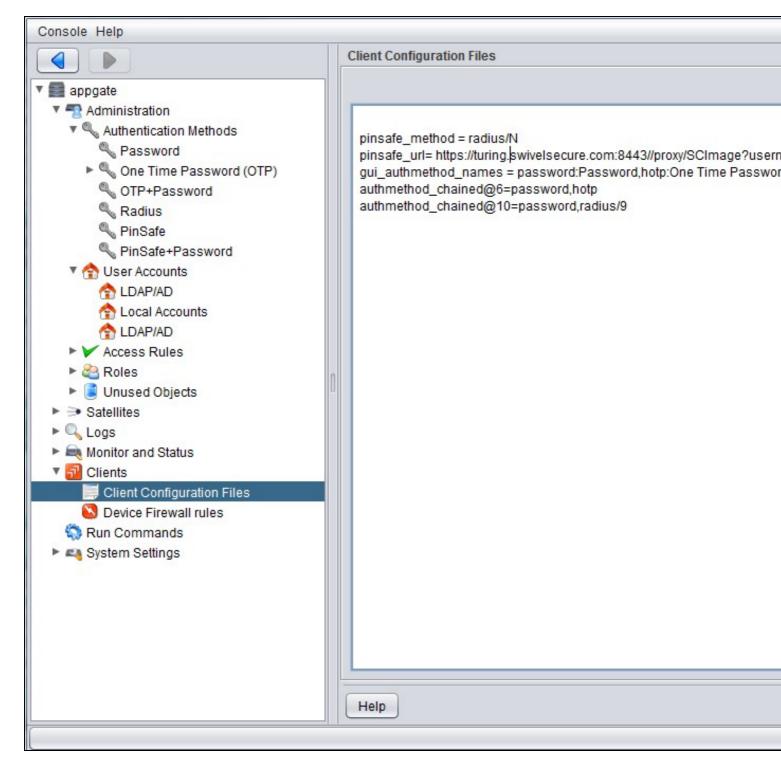
On the AppGate Security Server select Administration/Clients then Client Configuration Files and add the following lines:

pinsafe_method = radius/N

pinsafe_URL = http://server:port//pinsafe/SCImage?username=%u

where server is the Swivel sever public NAT and port the port to the Swivel server, usually 443 for a Swivel appliance. For further informationn refer to

the AppGate Security Server documentation under RADIUS/Pinsafe.



Testing Additional Configuration Options Troubleshooting

Check the Swivel logs for Turing images and RADIUS requests.

Known Issues and Limitations

None

Additional Information

For assistance in Swivel installation and configuration please firstly contact your reseller and then email Swivel Secure support at support@swivelsecure.com