

Palo Alto Networks Integration

Contents

- 1 Introduction
- 2 Prerequisites
- 3 Baseline
- 4 Architecture
- 5 Swivel Configuration
 - ◆ 5.1 Configuring the RADIUS server
 - ◆ 5.2 Setting up the RADIUS NAS
 - ◆ 5.3 Enabling Session creation with username
- 6 Palo Alto Networks Configuration
 - ◆ 6.1 Create a RADIUS Server Profile
 - ◆ 6.2 Create an Authentication Profile
 - ◆ 6.3 Configure the GlobalProtect Portal to use Swivel RADIUS Authentication
 - ◆ 6.4 Configure the GlobalProtect Gateway to use Swivel RADIUS Authentication
- 7 Additional Configuration Options
 - ◆ 7.1 Challenge and Response with Two Stage Authentication
- 8 Testing
- 9 Troubleshooting
- 10 Known Issues and Limitations
- 11 Additional Information

Introduction

This document describes steps to configure a Palo Alto Networks Firewall with Swivel as the authentication server using RADIUS with SMS, [Mobile Phone Client](#), and [Taskbar Authentication](#). The solution is tested with a Palo Alto Networks GlobalProtect client.

Prerequisites

Palo Alto Networks Firewall

Palo Alto Networks documentation

Swivel 3.x, 3.5 or later for RADIUS groups

Baseline

Palo Alto Networks PA-2050

Palo Alto Networks Software 4.1.6

Palo Alto Networks GlobalProtect Client 1.14 and 1.15

Swivel 3.8

Architecture

The Palo Alto Networks makes authentication requests against the PINsafe server by RADIUS.

Swivel Configuration

Configuring the RADIUS server

Configure the RADIUS settings using the RADIUS configuration page in the Swivel Administration console by selecting RADIUS Server. To turn on RADIUS authentication set **Server Enabled** to YES. The Host or IP address is the interface which will accept RADIUS requests, leave this blank to allow RADIUS requests on any interface. (In this example the HOST IP is set to 0.0.0.0 which is the same as leaving it blank).

For troubleshooting RADIUS debug can be enabled together with the debug log option, see [Debug how to guide](#)

Note: for appliances, the Swivel VIP should not be used as the server IP address, see [VIP on PINsafe Appliances](#)

RADIUS>Server

Please enter the details for the RADIUS server.

Server enabled:	<input type="text" value="Yes"/>
IP address:	<input type="text" value="0.0.0.0"/>
Authentication port:	<input type="text" value="1812"/>
Accounting port:	<input type="text" value="1813"/>
Maximum no. sessions:	<input type="text" value="50"/>
Permit empty attributes:	<input type="text" value="No"/>
Filter ID:	<input type="text" value="No"/>
Additional RADIUS logging:	<input type="text" value="Both"/>
Enable debug:	<input type="text" value="Yes"/>
Radius Groups:	<input type="text" value="Yes"/>
Radius Group Keyword:	<input type="text" value="POLICY"/>
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

Setting up the RADIUS NAS

Set up the NAS using the Network Access Servers page in the PINsafe Administration console. Enter a name for the VPN server. The IP address has been set to the IP of the VPN appliance, and the secret ?secret? assigned that will be used on both the PINsafe server and VPN RADIUS configuration.

RADIUS>NAS

Please enter the details for any RADIUS network access servers. A NAS is permitted to access the authentication via the RADIUS interface.

NAS: Identifier:	<input type="text" value="Device Name"/>
Hostname/IP:	<input type="text" value="192.168.0.1"/>
Secret:	<input type="password" value="•••••"/>
EAP protocol:	<input type="text" value="None"/>
Group:	<input type="text" value="---ANY---"/>
Authentication Mode:	<input type="text" value="All"/>
Change PIN warning:	<input type="text" value="No"/>
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

You can specify an EAP protocol if required, others CHAP, PAP and MSCHAP are supported. All users will be able to authenticate via this NAS unless authentication is restricted to a specific repository group.

Enabling Session creation with username

The Swivel server can be configured to return an image stream containing a TURING image in the [Taskbar](#)

Go to the ?Single Channel? Admin page and set ?Allow Session creation with Username:? to YES.

To test your configuration you can use the following URL using a valid Swivel username:

Appliance

https://Swivel_server_IP:8443/proxy/SCImage?username=testuser

For a software only install see [Software Only Installation](#)

Palo Alto Networks Configuration

Create a RADIUS Server Profile

On the Palo Alto Networks Administration console select the Device tab then Server Profiles and then RADIUS, and click on Add.

RADIUS Server Profile

Name: PINsafe

☐ Administrator Use Only

Domain:

Timeout: 3

Retries: 3

☐ Retrieve user group

Servers

Server	IP Address	Secret	Port
PINsafe	10.0.20.11	*****	1812

+ Add - Delete

OK Cancel

Enter the following information:

Name Descriptive name for the authentication server

Domain A domain to be appended to the authentication request

IP address or hostname of the Swivel server

Shared secret as entered on the PINsafe server

Port usually 1812 by default

The screenshot shows the Palo Alto Networks Administration console. The top navigation bar includes tabs for Dashboard, ACC, Monitor, Policies, Objects, Network, and Device. The left sidebar contains a tree view of configuration options, with RADIUS selected under Server Profiles. The main content area displays a table with columns for Name, Location, and Servers. A single entry, 'Swivel Radius', is listed with its location and server details. At the bottom of the table are buttons for Add, Delete, and Clone. The user 'swivel' is logged in.

Name	Location	Servers
Swivel Radius		Name: Swivel IP: 10.0.20.11 Port: 1812

Create an Authentication Profile

On the Palo Alto Networks Administration console select the Device tab then Authentication profiles, and click on New. Enter a name and select RADIUS as the authentication type, and the Swivel server for the profile.

The 'New Authentication Profile' dialog box is shown. The 'Profile Name' field contains 'Swivel'. Under the 'Lockout' section, 'Failed Attempts' is set to 10 (range 0-10) and 'Lockout Time' is set to 5 (range 0-60 mins). The 'Allow List' section has the 'All' checkbox checked. Below this are two empty list boxes for 'User Groups' and 'Users', with an 'Edit Allow List' button to the right. The 'Authentication' dropdown is set to 'RADIUS' and the 'Server Profile' dropdown is set to 'PINsafe'. 'OK' and 'Cancel' buttons are at the bottom right.

paloalto NETWORKS

Dashboard ACC Monitor Policies Objects Network **Device**

Config
 HIP Match
 Alarms
 Manage Logs
 Server Profiles
 SNMP Trap
 Syslog
 Email
 RADIUS
 LDAP
 Kerberos
 Local User Database
 Users
 User Groups
Authentication Profile
 Authentication Sequence
 Client Certificate Profile
 Scheduled Log Export
 Software
 SSL-VPN Client
 GlobalProtect Client
 Dynamic Updates
 Licenses
 Support
 Master Key and Diagnostics

Lockout						
	Name	Failed Attempts (#)	Time (mins)	Allow List	Authentication	Service
<input type="checkbox"/>	Local			all	Local	
<input type="checkbox"/>	Swivel	10	5	all	RADIUS	PINs

New... Delete Clone

swivel | Logout

Configure the GlobalProtect Portal to use Swivel RADIUS Authentication

On the Palo Alto Networks Administration console select the Network tab then SSL-VPN, either edit an existing GlobalProtect Portal or configure a new one by clicking on New.

Configure the **Authentication Profile** to use the authentication profile created above.

Add/Edit SSL VPN

General

Name: pinsafe

Client Configuration

Authentication Profile: Swivel
 Server Certificate: Portal1
 Client Certificate Profile: None
 Custom Login Page: None
☐ Redirect HTTP traffic to HTTPS login page

Interface Settings

Tunnel Interface: tunnel.1
 Max User: 10
☒ Enable IPsec

Gateway Address

Interface: ethernet1/1
 Choice: IP 192.168.1.1

Timeout Configuration

Login Lifetime: Days 3
 Inactivity Logout: Hours 3

OK Cancel

Configure the GlobalProtect Gateway to use Swivel RADIUS Authentication

On the Palo Alto Networks Administration console select the Network tab then SSL-VPN, either edit an existing GlobalProtect Gateway or configure a new one by clicking on New.

Configure the **Authentication Profile** to use the authentication profile created above.

The screenshot shows the 'GlobalProtect Gateway' configuration page in the Palo Alto Networks Administration console. The left sidebar contains three tabs: 'General', 'Client Configuration', and 'HIP Notification'. The main content area is divided into several sections:

- Name:** SSL-GW
- Authentication:**
 - Server Certificate: Gateway
 - Authentication Profile: [Red box around the dropdown menu]
 - Client Certificate Profile: GlobalProtect-Cert-Profile
- Timeout Configuration:**
 - Login Lifetime: Days, 30
 - Inactivity Logout: Hours, 2
- Tunnel Gateway Address:**
 - Interface: ethernet1/1
 - IP Address: [Empty field]

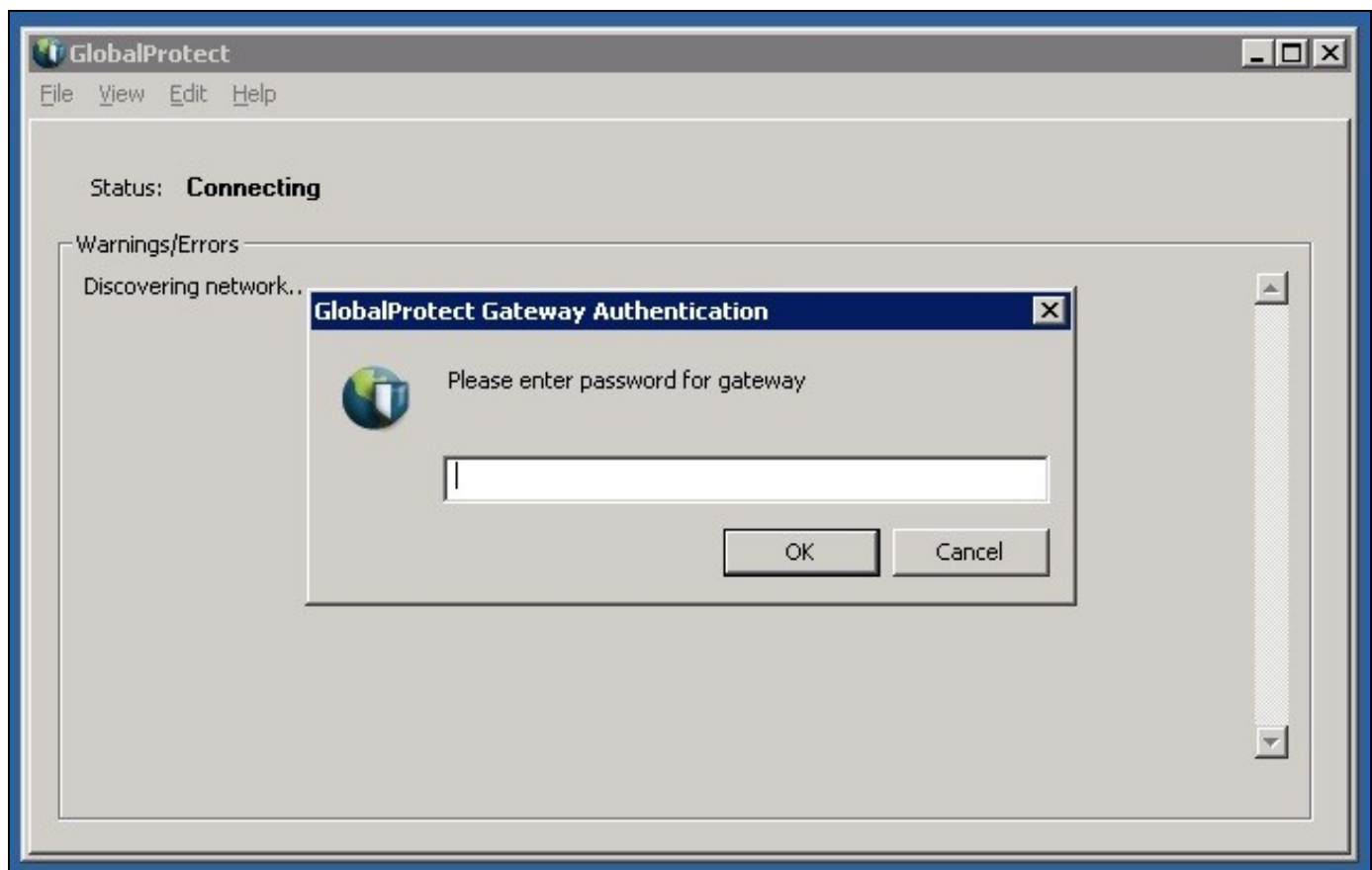
On the right side, there are additional options including a checked 'Tunnel M' checkbox, 'Tunnel Interface', 'Max U', 'Group Na', 'Group Passw', and 'Confirm Gro Passw'.

Additional Configuration Options

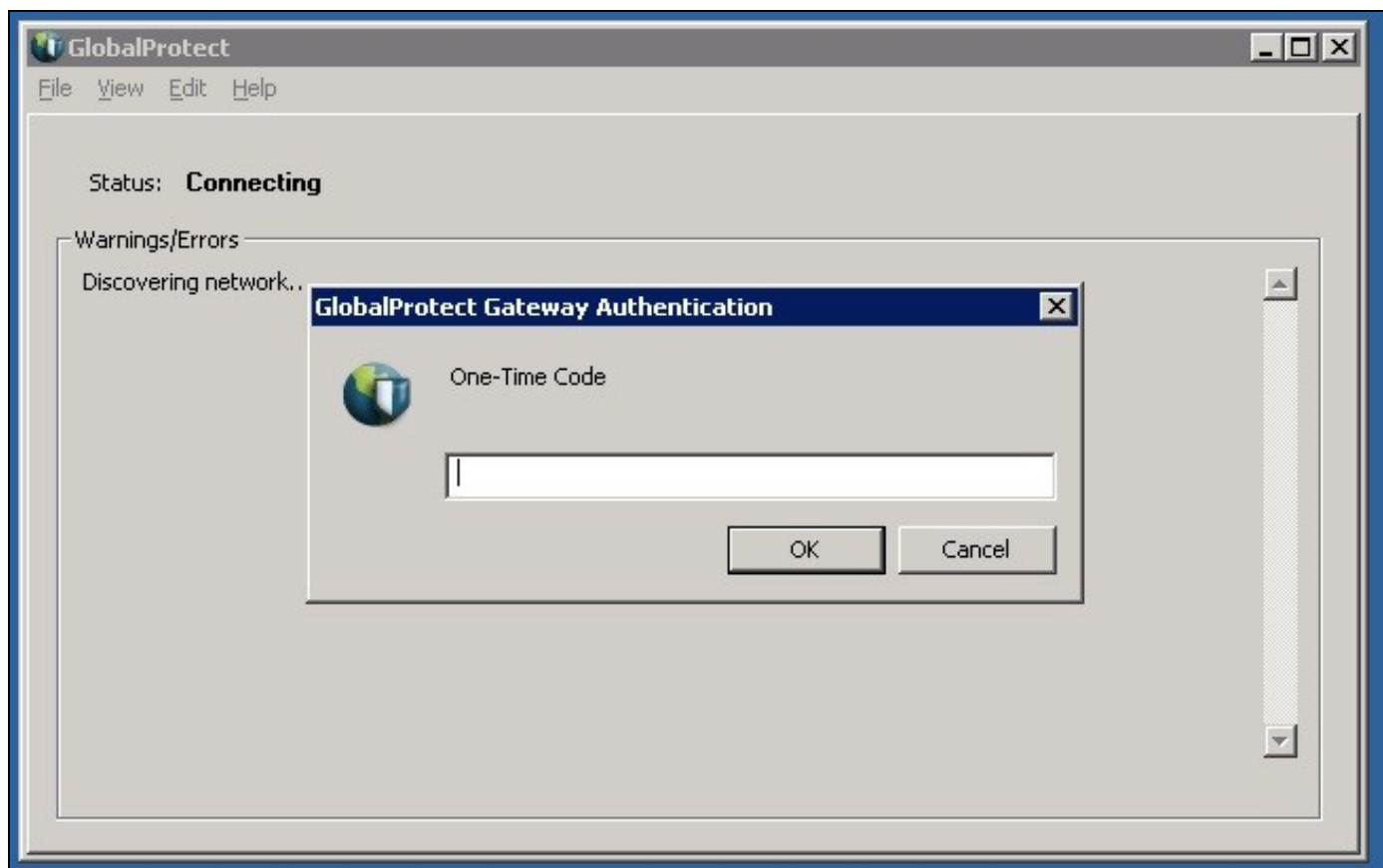
Challenge and Response with Two Stage Authentication

Challenge and Response is supported by using Two Stage authentication and Check Password with Repository using RADIUS PAP authentication. See [Challenge and Response How to Guide](#).

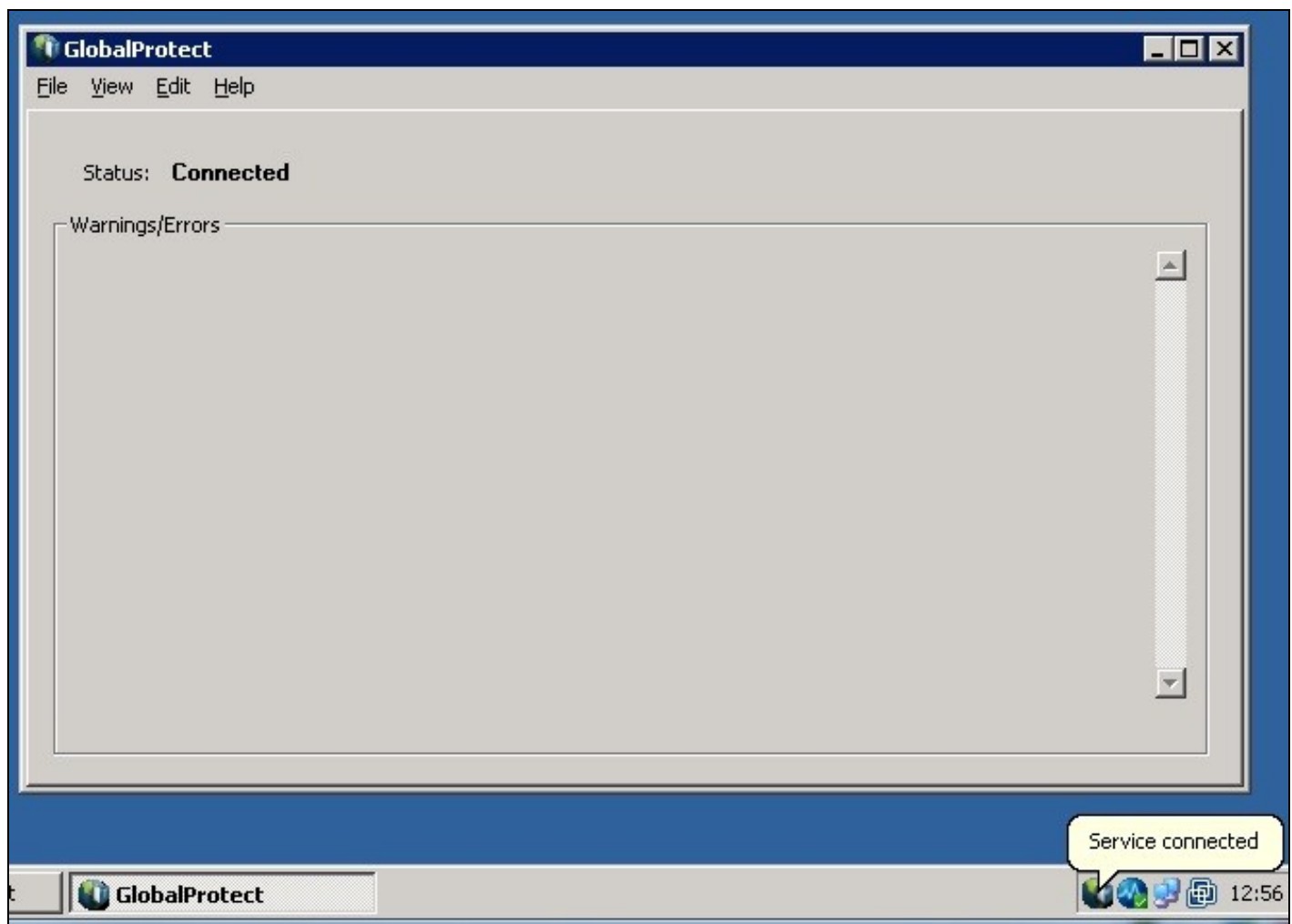
Enter Password



Enter OTC



IF OTC is correct then connection will be established



Testing

Connect to the GlobalProtect Client and authenticate using RADIUS authentication.

Troubleshooting

Check the PINsafe logs for RADIUS requests.

Known Issues and Limitations

None

Additional Information

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