DIGIPASS Authentication for Check Point Security Gateways

With IDENTIKEY Server

Integration Guideline
Disclaimer

Disclaimer of Warranties and Limitations of Liabilities
This Report is provided on an 'as is' basis, without any other warranties, or conditions.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of VASCO Data Security.

Trademarks
DIGIPASS & VACMAN are registered trademarks of VASCO Data Security. All trademarks or trade names are the property of their respective owners. VASCO reserves the right to make changes to specifications at any time and without notice. The information furnished by VASCO in this document is believed to be accurate and reliable. However, VASCO may not be held liable for its use, nor for infringement of patents or other rights of third parties resulting from its use.

Copyright
© 2009 VASCO Data Security. All rights reserved.
# Table of Contents

DIGIPASS Authentication for Check Point Security Gateways .......................... 1

Disclaimer ...................................................................................................... 2

Table of Contents ............................................................................................ 3

1 Overview ................................................................................................... 5

2 Problem Description .................................................................................. 5

3 Solution .................................................................................................... 5

4 Technical Concept ..................................................................................... 6

4.1 General overview .................................................................................. 6

4.2 4.2 Check Point Remote Access Methods .............................................. 6

4.3 Check Point Security Gateway prerequisites ......................................... 7

4.4 IDENTIKEY Server Prerequisites ........................................................... 7

5 Check Point Configuration ......................................................................... 8

5.1 General configuration ............................................................................. 8

5.1.1 RADIUS Configuration ...................................................................... 8

5.1.2 User Configuration ............................................................................ 11

5.1.3 Usergroup Configuration .................................................................. 12

5.1.4 Change Server Configuration ............................................................ 13

5.2 VPN Authentication .............................................................................. 14

5.3 Configure Office Mode .......................................................................... 15

5.4 Firewall Authentication .......................................................................... 16

5.5 Apply Changes ...................................................................................... 24

6 IDENTIKEY Server ................................................................................... 26

6.1 Policy configuration .............................................................................. 26

6.2 Client configuration .............................................................................. 29

7 SSL VPN test ........................................................................................... 31

7.1 SSL/VPN Authentication ....................................................................... 31
7.1.1  Response Only ...........................................................................31
7.1.2  Challenge / Response .................................................................32
7.2   Firewall Authentication .................................................................34
   7.2.1  Response Only .......................................................................34
   7.2.2  Challenge / Response ...............................................................37
8  About VASCO Data Security ..............................................................38
1 Overview

The purpose of this document is to demonstrate how to configure IDENTIKEY Server to work with Check Point firewall and VPN Security Gateways. Authentication is arranged on one central place where it can be used in a regular VPN or SSL/VPN connection or through the firewall rules that can request user authentication.

2 Problem Description

The basic working of Check Point firewall and VPN is based on authentication to an existing media (LDAP, RADIUS, local authentication ...). To use the IDENTIKEY Server with Check Point Security Gateways, the external authentication settings need to be changed or added manually.

3 Solution

After configuring IDENTIKEY Server and Check Point in the right way, you eliminate the weakest link in any security infrastructure – the use of static passwords – that are easily stolen guessed, reused or shared.

In this integration guide we will make use of a Check Point UTM installation. This combines a firewall, an IPSec or SSL/VPN and a UTM suite in one. For authentication, we focused on the SSL/VPN and the firewall part.
4 Technical Concept

4.1 General overview

The main goal of the Check Point Security Gateway is to perform authentication to secure all kind of VPN and firewall connections. As the Security Gateway can perform authentication to an external service using the RADIUS protocol, we will place the IDENTIKEY Server as back-end service, to secure the authentication with our proven IDENTIKEY Server software.

4.2 Check Point Remote Access Methods

Every enterprise has unique requirements for remote access. Check Point Security Gateways provide flexibility to design a solution to meet your needs.

- Check Point Endpoint Security— Check Point Endpoint Security™ is the first single agent for total endpoint security that combines the highest-rated firewall, network access control (NAC), program control, antivirus, anti-spyware, data security, and remote VPN access.

- Endpoint Connect™ VPN Client - Endpoint Connect provides mobile users with seamless, LAN-like secure remote access to corporate network resources and information.

- SecureClient Mobile—SecureClient Mobile delivers firewall protection and secure, uninterrupted remote access for wireless devices such as mobile phones

- SSL Network Extender—SSL Network Extender™ is an on-demand client that provides full network-layer secure access through a browser plug-in, enabling remote users to access email or other network applications in their native interfaces.

This guide provides an example configuration using SSL Network Extender, a SSL VPN remote access solution, and on firewall user authentication.
4.3 Check Point Security Gateway prerequisites

Please make sure you have a working setup of a Security Gateway. It is very important this is working correctly before you start implementing the authentication to the IDENTIKEY Server.

At this time this is a list of products that are supported to use authentication and can be managed with Check Point Security Management server:

- Firewall
- IPsec VPN

- UTM-1
- POWER-1
- IP Appliances

- VPN-1 UTM Edge

Current version: R70

These are appliance versions (current version: R70)

This also has a stand-alone management tool.

The products mentioned above are each available for different platforms. The Security Management server is available for SecurePlatform, Red Hat, Windows and Solaris.

4.4 IDENTIKEY Server Prerequisites

In this guide we assume you already have IDENTIKEY Server installed and working. If this is not the case, make sure you get IDENTIKEY Server working before installing any other features.
5 Check Point Configuration

5.1 General configuration

In this chapter you will learn how to configure an external RADIUS authentication server, our IDENTIKEY Server. This server will then be used in different applications.

When talking about the tabs in the left window, we refer to this tab bar.

5.1.1 RADIUS Configuration

Let’s start with creating the RADIUS configuration in the SmartDashboard. Open SmartDashboard and on the tabs in the left window select the Servers and OPSEC Applications tab. Right-click Servers and select RADIUS...

Figure 2: RADIUS Configuration (1)
We will create an external RADIUS server. To do that, we will first create a host where the IDENTIKEY Server is located. Click the **New...** button behind the Host field.

**Figure 3: RADIUS Configuration (2)**

Type in the **name** and the **IP address** from the IDENTIKEY Server. If you type in a resolvable hostname (FQDN or NetBios) you can click the Get address button to resolve the hostname to the IP address. When done, click **OK**.

**Figure 4: RADIUS Configuration (3)**
Back in the first screen, your host will now be filled in automatically with the one you just created. Enter a **Name** and **Shared Secret**.

**RADIUS version 2.0** is necessary to enable all features for IDENTIKEY Server.

- e.g. PIN change = passwords larger than 16 characters
  - Password+PIN+OTP+NewPIN+NewPIN
  
Passwords larger than 16 characters are cut off after the 16th character if RADIUS version 1.0 is used.

As **Service** it depends on which port you installed IDENTIKEY Server.

1812 = NEW-RADIUS
1645 = RADIUS

![RADIUS Configuration](image)

**Figure 5: RADIUS Configuration (4)**

Click OK when finished. You will now see the RADIUS server in the list. You can still edit this server by right-clicking the object and selecting **Edit**. The host you created can be found in the Network Objects tab, under Nodes.
5.1.2 User Configuration

We will now create a method so users will be authenticated through the newly created RADIUS server. Go to the Users tab and right click External User Profiles and select New External User Profile → Match all users...

![Figure 6: User Configuration (1)](image)

On the Authentication tab, select RADIUS as Authentication Scheme. As a RADIUS server select the newly created RADIUS server pointing to IDENTIKEY Server.

![Figure 7: User Configuration (2)](image)

![Figure 8: User Configuration (3)](image)
5.1.3 Usergroup Configuration

We will now create a group for the generic* RADIUS user to work with. Only groups can be used in the rules to allow access.

In the same user tab, right-click **User Groups → New Group**.

![Figure 9: Usergroup Configuration (1)](image)

Fill in the RADIUS Group **Name** and move the **generic* RADIUS** user to the **In Group** list.

![Figure 10: Usergroup Configuration (2)](image)
5.1.4 Change Server Configuration

To make sure the Check Point Security Gateway is configured correctly for RADIUS authentication we will check its general configuration in the following chapter.

Go to the Network Objects tab and select your Security Gateway from the Check Point list.

Right-click your server and select **Edit...**

![Figure 11: Change Server Configuration (1)](image)

In this case we only want to allow users to make a VPN connection when they verify themselves with a One Time Password to our IDENTIKEY Server.

Go to the **Remote Access** → **Office Mode** and select **Offer office mode to group:** and select your **RADIUS group** you recently created.

![Figure 12: Change Server Configuration (2)](image)
5.2 VPN Authentication

In this chapter we will show you how to use the RADIUS authentication to make an SSL VPN connection.

Go to the VPN Communities tab and right-click the Remote Access → RemoteAccess and select Edit...

**Figure 13: VPN Authentication (1)**

Select the Participant User Group and add the RADIUS group to this list.

**Figure 14: VPN Authentication (2)**

Note: SSL Network Extender uses TCP 443. Ensure this does not conflict with the port used to manage the Check Point Security Gateway.
5.3 Configure Office Mode

Select Remote Access > Office Mode and configure it as needed. For more information refer to the Check Point VPN Administration Guide. Identikey does not support obtaining an Office Mode IP address via RADIUS.

Configure the Security Gateway to support SSL Network Extender

Select Remote Access > VPN Clients and activate Support SSL Network Extender.

Select the server side certificate with which the gateway will authenticate from the drop-down list.

Install the policy.
5.4 Firewall Authentication

In this chapter we will show you how to protect a firewall rule by using the external RADIUS server and so require the use of OTP's.

First, make sure you are in the Firewall (Security) tab (1). Select one of the rules you see in the list. Then, click the button to add a firewall rule below the current one.(2)

A new rule will appear, with an empty Name-field. Double click the empty Name-field.

![Figure 15: Firewall Authentication (1)](image)

Give the new rule a **Name** and click **OK**.

![Figure 16: Firewall Authentication (2)](image)
In the **Source** field, we will enter the group that has access to the website we will be publishing. Right-click this field and choose **Add User Access...**

![Image](image.png)

**Figure 17: Firewall Authentication (3)**

Select the **RADIUS group** you created earlier, check the **No restriction** option and click **OK**.

![Image](image.png)

**Figure 18: Firewall Authentication (4)**
For the **Destination**, right-click the field and choose **Add...**

![Figure 19: Firewall Authentication (5)](image)

If the server that hosts your website is not in the list, click the **New...** button and select **Node → Host...**

![Figure 20: Firewall Authentication (6)](image)
Fill in the **Name** and the **IP Address**. If the Name is an FQDN or Netbios host, you can click the Get address button to resolve the IP Address. When done, click **OK**.

![Host Node - DC](image)

**Figure 21: Firewall Authentication (7)**

You will now find the newly created host in the list, select it and click **OK**.

![Add Object](image)

**Figure 22: Firewall Authentication (8)**
There are only three services supported for user authentication: HTTP, FTP and Telnet.

In this firewall rule we only want to allow HTTP traffic. Right-click the **Service** field and select **Add...**

**Figure 23: Firewall Authentication (9)**

Choose **http** from the list and click **OK**.

**Figure 24: Firewall Authentication (10)**
To request user authentication, right-click the **Action** field and select **Client Auth** from the list.

![Figure 25: Firewall Authentication (11)](image)

Instead of Client Authentication there are 2 other possibilities, a little more information about this field type:

**User Authentication:**

User authentication grants access on a per-user basis. This method can only be used for telnet, ftp, rlogin, http and https, and requires separate authentication for each connection.

User Authentication is secure, because the authentication is valid only for one connection, but intrusive, because each connection requires another authentication. For example, accessing a single web page could display several dozen User Authentication windows, as different components are loaded.

**Session Authentication:**

Session Authentication is not like user authentication because it requires authentication for each session, and can be used with any service. Session authentication is secure, but requires a session authentication agent to be running on the authentication client, or on another machine in the network. Session authentication can be used to authenticate any service on a per-session basis. After the user initiates a connection directly to the server, the security gateway - located between the user and the destination - intercepts the connection. The gateway recognizes that user-level authentication is required, and initiates a connection with a session authentication agent.

The session authentication agent is a utility provided with VPN-1 NGX, and must be installed on any object running session authentication. The Agent performs required authentication, which allows connections to continue to the requested server, if permitted.
Client Authentication:

Client authentication grants access on a per-host basis. Client authentication allows connections from a specific IP address, after successful authentication. It can be used for any service, for any number of connections and the authentication is valid for the length of time specified by the administrator. It is slightly less secure than user authentication, because it allows any user access from the IP address or host, but is also less intrusive than session authentication. Client authentication is best used when the client is a single-user machine, such as a PC.

It is best practice to enable "specific sign on" in the properties of the client authentication method. If specified, only connections that match the original connection are allowed without additional authentication. If a rule specifies more than one service or host, the user on the client must re-authenticate for each service or host. Specific Sign On is useful if you want to limit access to services and target hosts.

If you choose Manual, you have to authenticate by making a telnet connection to the firewall on port 259 or by browsing to http://<firewall>:900.
Finally, to change the authentication settings, right-click the **Client Auth** field and select **Edit Properties**...

![Client Authentication Window](image)

**Figure 26: Firewall Authentication (12)**

In the Source box, select **ignore user database**. As Required Sign On select **Standard** and change the Sign On Method to **Fully automatic**. Click OK to continue.

![Client Authentication Window](image)

**Figure 27: Firewall Authentication (13)**

We now created a firewall rule allowing the firewall to request user authentication before accessing a website. We also changed the VPN settings sending the user credentials to the external RADIUS server. Both ways will make use of the IDENTIKEY Server to perform authentication, allowing you to make use of DIGIPASS One Time Passwords.
5.5 Apply Changes

The Security Management server is only a dashboard to show the configuration of the Check Point software. We still have to save all changes and install the policy to deploy the changes to the Security Gateways.

Click **Policy → Install...** to deploy all the changes to the Security Gateway.

![Figure 28: Apply Changes (1)](image)

You will receive the question to which Check Point target you want to deploy the changes. In our case, “member” is the name of our Security Gateway server.

Select the correct **Installation Target** and click **OK**.

![Figure 29: Apply Changes (2)](image)
Once the installation of the policy has finished, click **Close**.

![Figure 30: Apply Changes (3)](image)

We have now configured the Check Point Security Gateway so that VPN and firewall connections will be protected by the Vasco IDENTIKEY Server. This allows you to make use of OTP’s in different places of the Security Gateway.

We will now show how IDENTIKEY Server has to be configured. Next we will look into the end-users experience when using a DIGIPASS to logon.
6 IDENTIKEY Server

Go to the IDENTIKEY Server web administration page, and authenticate with an administrative account.

6.1 Policy configuration

To add a new policy, select Policies > Create.

There are some policies available by default. You can also create new policies to suit your needs. Those can be independent policies or inherit their settings from default or other policies.
Fill in a policy ID and description. Choose the option most suitable in your situation. If you want the policy to inherit setting from another policy, choose the right policy in the Inherit From list. Otherwise leave this field to None.

Figure 32: Policy configuration (2)

In the policy options configure it to use the right back-end server. This could be the local database, but also active directory or another radius server.

This is probably the same that was in your default client authentication options before you changed it. Or you use the local database, Windows or you go further to another radius server.

In our example we select our newly made Demo Policy and change it like this:

- **Local auth.**: Digipass/Password
- **Back-End Auth.**: Default (None)
- **Back-End Protocol**: Default (None)
- **Dynamic User Registration**: Default (No)
- **Password Autolearn**: Default (No)
- **Stored Password Proxy**: Default (No)
- **Windows Group Check**: Default (No Check)

After configuring this Policy, the authentication will happen locally in the IDENTIKEY Server. So user credentials are passed through to the IDENTIKEY Server, it will check these credentials to its local user database and will answer to the client with an Access-Accept or Access-Reject message.
In the Policy tab, click the **Edit** button, and change the **Local Authentication** to **Digipass/Password**.

*Figure 33: Policy configuration (3)*

The user details can keep their default settings.

*Figure 34: Policy configuration (4)*
6.2 Client configuration

Now create a new component by right-clicking the Components and choose **New Component**.

![Figure 35: Client configuration (1)](image-url)
As component type choose **RADIUS Client**. The location is the **IP address** of the client. In the policy field you should find your **newly created policy**. Fill in the **shared secret** you entered also in the client for the RADIUS options. In our example this was “vasco”. Click **Create**.

![Client configuration](image)

**Figure 36: Client configuration (2)**

Now the client and the IDENTIKEY Server are set up. We will now see if the configuration is working.
7 SSL VPN test

7.1 SSL/VPN Authentication

First we will test the SSL/VPN functionality, with Response Only and Challenge/Response.

7.1.1 Response Only

Going to https://<ip_or_FQDN_VPN-1 server>, will show you an SSL/VPN login screen. Enter your **Username**, in the **Password**-field enter the DIGIPASS OTP and click **OK**.

*In our case the url was https://checkpoint.vpn-1.utm.*

Figure 37: SSL/VPN Authentication – Response Only (1)

After verifying the credentials successfully, we are authenticated to start the SSL/VPN connection.

Figure 38: SSL/VPN Authentication – Response Only (2)
7.1.2 Challenge / Response

Now let’s take a look at the challenge/response method.

Type in a **username** and **password (or keyword)** to trigger the challenge code and click **OK**.

![SSL Network Extender](image1)

**Figure 39: SSL/VPN Authentication – Challenge / Response (1)**

Now, on top of the screen, you will see a **DP300 Challenge** code.

Use this challenge to generate a **response** using a DIGIPASS with challenge/response functionality. Fill in the generated response in the corresponding box and click **OK** to authenticate.

![SSL Network Extender](image2)

**Figure 40: SSL/VPN Authentication – Challenge / Response (2)**

When using the challenge/response method, you will receive a message box stating you authenticated by RADIUS authentication. Click **OK** to continue.

![Windows Internet Explorer](image3)

**Figure 41: SSL/VPN Authentication – Challenge / Response (3)**
Then again you will receive the connection window with all details about your VPN connection.

![SSL Network Extender](image)

**Figure 42: SSL/VPN Authentication – Challenge / Response (4)**
7.2 Firewall Authentication

We will now take a look at the firewall authentication part. We try to reach the initial web page from IIS on the DC server.

7.2.1 Response Only

We have two options to perform our authentication. We could make a telnet connection to the firewall on port 259 or we browse to http://<firewall>:900. We choose to make use of the web-service to authenticate.

Browse to http://<firewall>:900, and enter your username. Click Submit.

In our case this is http://checkpoint.vpn-1.utm:900.

Figure 43: Firewall Authentication – Response Only (1)
Enter your **password** (One Time Password) and click Submit.

**Figure 44: Firewall Authentication – Response Only (2)**

The method depends on the selection you made in the properties of the client authentication. We selected **Standard Sign-on**, so we select this option and click Submit.

**Figure 45: Firewall Authentication – Response Only (3)**
If the authentication succeeds you will receive a confirmation message on screen.

Figure 46: Firewall Authentication – Response Only (4)

We will now be authorized to browse to the specified page we initially wanted to secure: http://cp.labs.vasco.com. And indeed, we are shown the initial page from IIS.

Figure 47: Firewall Authentication – Response Only (5)
7.2.2 Challenge / Response

The method for challenge/response is exactly the same as above. You will only receive one screen extra after entering your static password in the password field. The screen with the challenge shown on the screen and an extra input field to enter your response.

Figure 48 Firewall Authentication – Challenge/Response (1)
8 About VASCO Data Security

VASCO designs, develops, markets and supports patented Strong User Authentication products for e-Business and e-Commerce.

VASCO’s User Authentication software is carried by the end user on its DIGIPASS products which are small “calculator” hardware devices, or in a software format on mobile phones, other portable devices, and PC’s.

At the server side, VASCO’s VACMAN products guarantee that only the designated DIGIPASS user gets access to the application.

VASCO’s target markets are the applications and their several hundred million users that utilize fixed password as security.

VASCO’s time-based system generates a “one-time” password that changes with every use, and is virtually impossible to hack or break.

VASCO designs, develops, markets and supports patented user authentication products for the financial world, remote access, e-business and e-commerce. VASCO’s user authentication software is delivered via its DIGIPASS hardware and software security products. With over 25 million DIGIPASS products sold and delivered, VASCO has established itself as a world-leader for strong User Authentication with over 500 international financial institutions and almost 3000 blue-chip corporations and governments located in more than 100 countries.