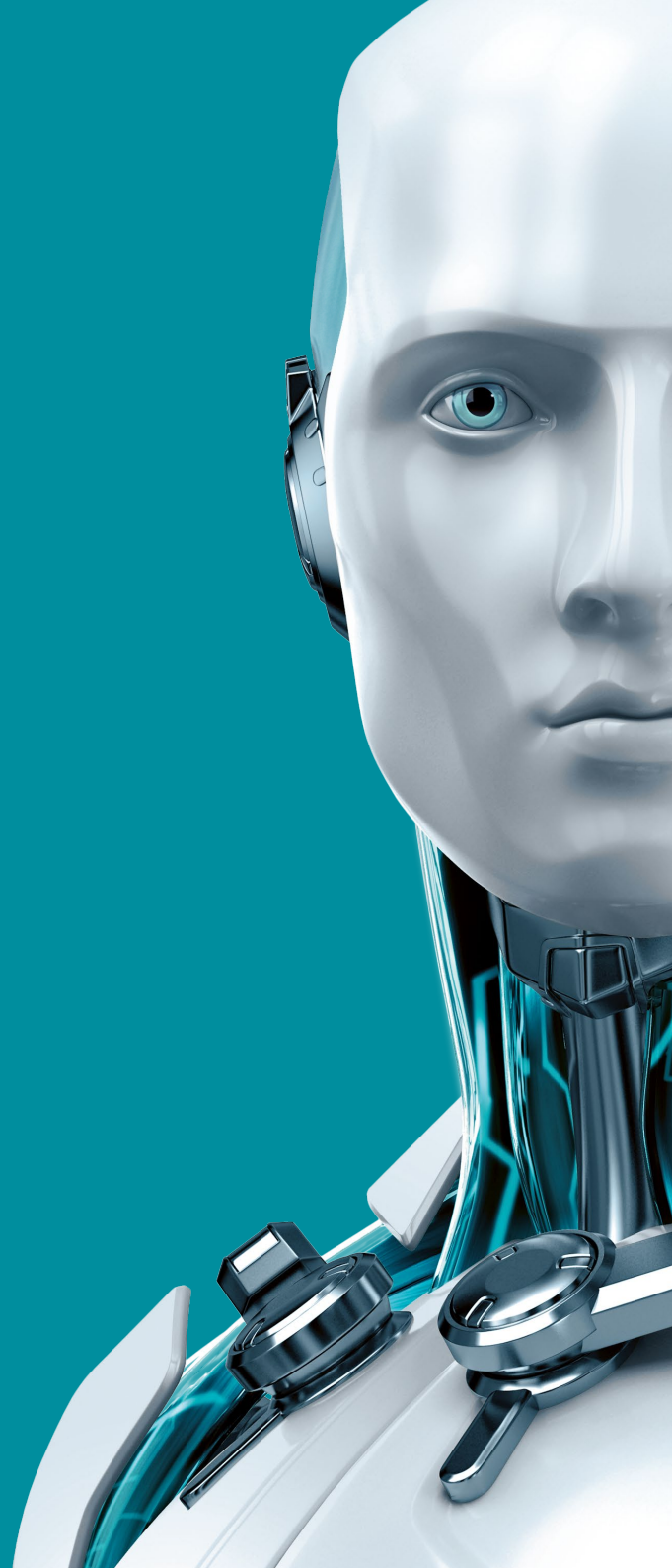
SECURE AUTHENTICATION

Keeping your VPN protected

BUSINESS

ENJOY SAFER TECHNOLOGY™



SECURE AUTHENTICATION

ESET Secure Authentication helps businesses to make access to their data secure. Any organization can set up ESET's two-factor authentication in just 10 minutes – and thus easily reduce the risk of data breaches, caused by stolen, weak or compromised passwords.

The solution consists of the server side and the client side – the latter comes in the form of a mobile app. The authentication options include Push Authentication, as well as generating and delivering one-time passwords (OTPs) via the mobile app, but also via SMS messages or your organization's existing hardware tokens.

Overview

The increasing use of remote access is driving businesses to look for an easy to manage, secure solution for providing access to sensitive company assets.

There are a growing number of easy to configure and affordable VPN solutions offering both remote access and in some cases Unified Threat Management to companies of all sizes – from Small and Medium Businesses to Enterprises.

ESET with its NOD32® technology secures business IT infrastructure across all major operating systems. It now offers a way to provide strong authentication through this class of VPN device, using One Time Passwords (OTPs) generated by a simple-to-use app on the user's mobile phone.

ESET Secure Authentication combined with your VPN gives you easy and ultra secure remote access – everywhere and any time.

The Problem

Businesses are increasingly being asked to offer remote access to corporate applications and resources, whether by mobile workers, small branch locations or partners and customers. True network security requires multiple elements and many of these are provided via any of a growing range of VPN appliances.

However, as static passwords are widely known to be non-secure and easy to compromise, many security experts recommend supplementing the built-in user authentication of these devices by adding a second factor or strong authentication.

ESET Secure Authentication integrates with all major VPNs to provide two-factor user authentication, ensuring strong security for the corporate LAN and central resources.

Two-Factor Authentication (2FA) is an authentication method which requires two independent pieces of information to establish a user's identity. 2FA is much stronger than traditional password authen-tication, which requires only one factor.

This document presents an overview of how quick and easy configuration is for these devices.

Individual in-depth integration guides for each VPN device are available via the links at the end of this document or by searching the ESET Knowledge Base for the name of the VPN appliance.

The Solution

ESET Secure Authentication can be easily deployed to supplement existing VPN devices, adding strong authentication without any significant change to the VPN configuration.

The standard authentication method for the majority of VPN devices is based on either LDAP, RADIUS or local authentication. ESET Secure Authentication uses RADIUS as an external authentication method for your VPN device.

After configuring ESET Secure Authentication and your VPN correctly, you will have eliminated the weakest point of any security infrastructure – the use of static passwords, which are easily stolen, guessed, reused or shared.

Benefits

ESET Secure Authentication offers the following benefits in combination with your chosen VPN appliance:

1. Greatly enhanced security requiring two independent pieces of information for authentication
2. Reduced risks from weak passwords
3. Minimal time needed for training and supporting users
4. Easy to implement into your network

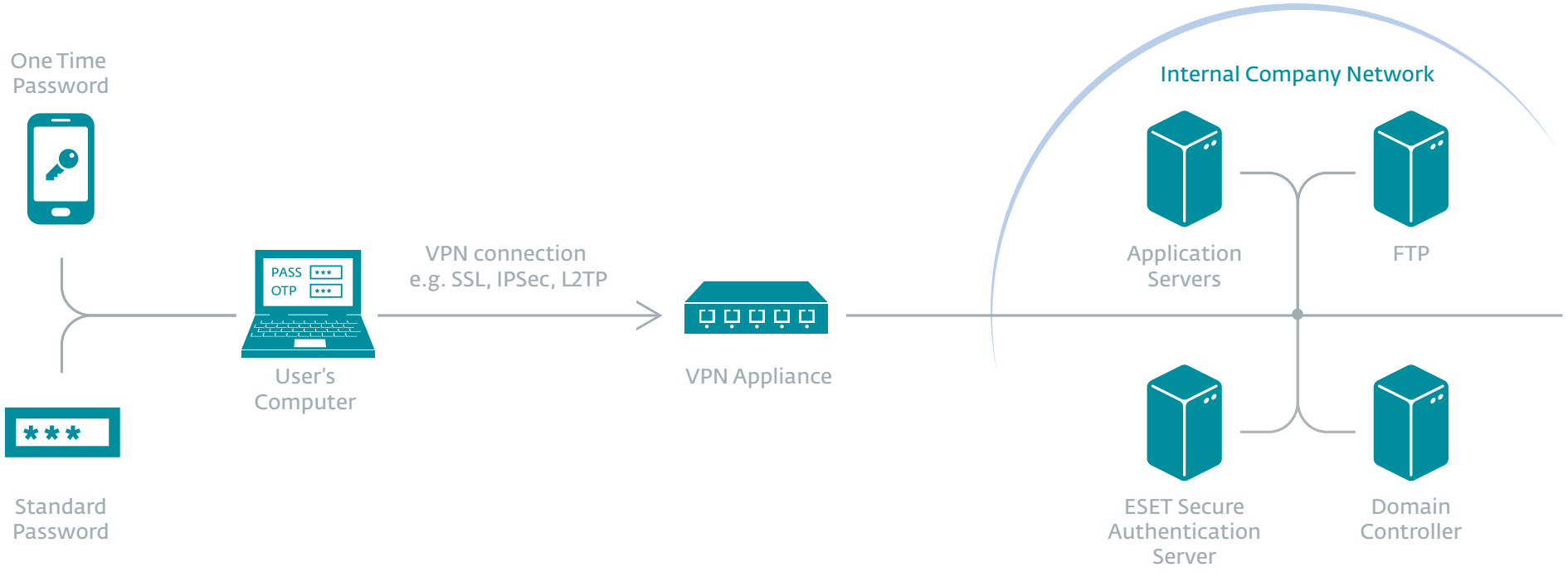
How does 2FA work with ESET Secure Authentication?

Two-Factor authentication requires the use of a third-party authentication service. The authentication service consists of two parts:

1. An ESET Secure Authentication RADIUS Server running in your Windows Network where an administrator can use Active Directory Users and Computers (ADUC) to configure users' 2FA settings.
2. A mobile application (for all mobile operating systems) running on the user's mobile phone, which is used to generate OTPs for each authentication attempt. Alternatively, OTPs can be delivered on-demand by SMS.

Once enabled for 2FA, a user must enter a valid OTP in addition to their static password to gain access. They receive these 6-digit codes from the app running on their mobile phone – codes which can be generated without the phone being connected to a network. The static password is forwarded via the VPN to the back end (Domain Controller) to verify that the static password is correct. The OTP is forwarded and checked against the ESET Secure Authentication Server running on the network. Only if both are correct is the user authenticated.

Your VPN with ESET Secure Authentication



Technical Specification

General Overview

RADIUS authentication with ESET Secure Authentication operates in the following way:

1. A remote user initiates a connection to the VPN
2. The VPN appliance gathers the user's ID, static password and OTP and submits these credentials to the ESET Secure Authentication RADIUS server
3. The server marshals the credentials to the ESET Secure Authentication Core Authentication Service
4. The Authentication Service authenticates the static password against AD, and the OTP against the secret data stored on the user's AD account
5. The VPN appliance then grants the authenticated user access to the company network

VPN authentication with ESET Secure Authentication

Your VPN's main purpose is to secure remote connections. It can perform the authentication for this against an external service using the RADIUS protocol – this allows the ESET Secure Authentication RADIUS Server to function as a back-end service for your VPN.

Users will be authenticated first by the ESET Secure Authentication Server, which can be linked to Active Directory in the back-end. In effect the ESET Secure Authentication Server is deployed in between the VPN and Active Directory.

This means that ESET Secure Authentication receives all authentication requests from your VPN. The OTP with the authentication requests will be verified by the ESET Secure Authentication RADIUS Server. The Server will relay the static password to the back-end (RADIUS Server or Active Directory) for verification if required. After a successful verification, a RADIUS ACCESS-ACCEPT message will be sent to the VPN for the authentication response.

Prerequisites for Securing your VPN with ESET Secure Authentication

VPN Prerequisites

A VPN with a working setup is an essential prerequisite for securing your VPN with ESET Secure Authentication. It is important that this is working correctly before you begin implementing ESET Secure Authentication.

Active Directory

Active Directory must already be set up – it will be used as the back-end authentication for users' static passwords. User accounts must also have been created in Active Directory.

ESET Secure Authentication Server

ESET Secure Authentication must be installed on the Active Directory Domain. ESET Secure Authentication ships with a standalone RADIUS server, so it has everything you need to add 2FA to your VPN.

Integration Guides

Guides are available on the ESET Knowledge base for:

Barracuda

Check Point Software

Cisco ASA IPsec

Cisco ASA SSL

Citrix Access Gateway

Citrix Netscaler

Citrix XenApp server

Cyberoam

F5 Firepass

Fortinet Fortigate

Juniper

Microsoft RRAS

Microsoft RRAS with NPS

Microsoft Forefront Threat Management Gateway

Netasq

OpenVPN Access Server

Palo Alto

Sonicwall

VMWare Horizon View

Copyright © 1992 – 2017 ESET, spol. s r. o. ESET, ESET logo, ESET android figure, NOD32, ESET Smart Security, SysInspector, ThreatSense, ThreatSense.Net, LiveGrid, LiveGrid logo and/or other mentioned products of ESET, spol. s r. o., are registered trademarks of ESET, spol. s r. o. Windows® is a trademark of the Microsoft group of companies. Other here mentioned companies or products might be registered trademarks of their proprietors. Produced according to quality standards of ISO 9001:2008.