How to Dialogue mode authentication using NetScaler OTP

Objective

This article describes how to configure NetScaler Gateway for Dialogue mode authentication using NetScaler OTP as one of the authentication factors.

Introduction

Time-based One-Time Passwords (OTP) are a way of authenticating users. It is called One-Time Password, since the password code changes each time. OTPs have transformed from being a hardware-based authentication device, to software based applications that can be installed on your smartphones. For implementing an OTP, customers need an OTP generator and an OTP validator. The OTP generator is what users have that displays the password, whilst validator is the one that verifies the one-time password generated by the user token. NetScaler Unified Gateway can now act as a validating server for OTP thus avoiding a need for an external third party server, thereby simplifying the network and helping reduce cost.

A dialogue mode authentication is an interactive way of authenticating users. For example, user is presented with a challenge to prove his/her identity. Based on the success criteria, user is presented with additional challenges before allowing access to resources.

In this article, we will configure dialogue mode authentication using LDAP as first factor authentication and NetScaler OTP as second factor authentication. User is first required to enter username and password for LDAP authentication. If successful, user is presented with another page to enter OTP. Even if this match, user is allowed access.

Following nFactor logic will be implemented.
Pre-requisites

It is assumed that following configurations are in place.
- VPN Vserver/Gateway and Authentication Vserver configurations
- LDAP server configurations and associated policies.

As part of this guide, the required policies and policy label configurations will be shown and bound to AAA vserver.

Note: To complete the configuration bind AAA vserver->Authentication Profile->VPN vserver (this is not part of this guide).

Policy and Policy Label mapping

Below graph shows mapping of policies and policy label.
Configuration Steps

Configurations steps below

1. Go to Security -> AAA – Application Traffic ->Policies->Authentication->Advanced Policies->Policy. Click Add. Choose Action Type LDAP and bind an existing LDAP policy. Use the following expression HTTP.REQ.COOKIE.VALUE("NSC_TASS").EQ("manageotp"). This policy will be the start of user management flow.

![Configure Authentication Policy](image1)

2. Similar to previous step add another policy ldap_otp. This policy will be start of User logon flow.

![Configure Authentication Policy](image2)
3. Similar to previous step add another policy `otp_manage_ldap`. This policy will be used for both registering/managing OTP devices and OTP authentication.

Note: Here `LDAP_no_auth` is a LDAP policy, with similar LDAP servers as configured previously, but with “Authentication” option unchecked and OTP Secret parameter configured with userparameters, as shown below.

   ![Authentication PolicyLabel]

Note: LSCHEMA_INT contains no_schema. Bind otp_manage_ldap policy created in step 3.

5. Similar to step 4, create another policy label OTP_Second_page and bind it with policy otp_manage_ldap.

   ![Authentication PolicyLabel]

Note: The OTP_Second_Factor schema is derived from OnlyPassword.xml schema. You can create this while configuring policy label and presented with option to choose a schema. At this step, create a new schema called OTP_Second_Factor as shown below.

- usch_ff
  HTTP.REQ.COOKIE.VALUE("NSC_TASS").EQ("manageotp")
  usch_firstfactor

- OTP_First
  true
  OTP_First_factor

Note: usch_ff expression HTTP.REQ.COOKIE.VALUE("NSC_TASS").EQ("manageotp").


Note

On your Unified Gateway’s Content switching policy you should have the following expression. Traffic Management -> Content Switching -> Virtual Servers -> <pick the vserver> -> Content Switching Policy Binding-> Content switching Policy.

```plaintext
is_vpn_url || HTTP.REQ.URL.CONTAINS("manageotp")
```

Additional Resources


Nfactor concepts: [https://support.citrix.com/article/CTX222713](https://support.citrix.com/article/CTX222713)

LDAP Authentication: [https://support.citrix.com/article/CTX108876](https://support.citrix.com/article/CTX108876)