How to configure pre-auth EPA scan as a factor in nFactor authentication

Objective

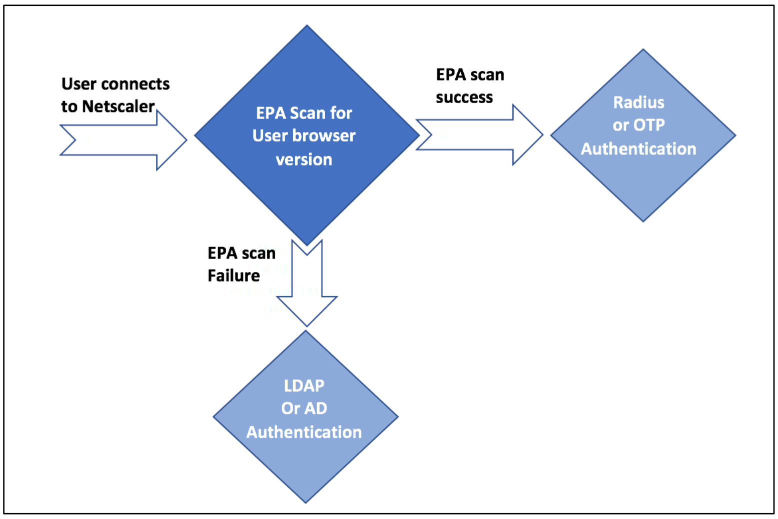
This article describes how to configure NetScaler Gateway for nFactor authentication with pre-auth EPA scan as one of the authentication factors.

Introduction

Multi-factor authentication enhances the security of an application by requiring users to provide multiple proofs of identify to gain access. The NetScaler appliance provides an extensible and flexible approach to configuring multi-factor authentication. This approach is called nFactor authentication

On NetScaler Gateway, End Point Analysis (EPA) can be configured to check if a user device meets certain security requirements and accordingly allow access of internal resources to the user. The Endpoint Analysis Plug-in downloads and installs on the user device when users log on to NetScaler Gateway for the first time. If a user does not install the Endpoint Analysis Plug-in on the user device or chooses to skip the scan, the user cannot log on with the NetScaler Gateway Plug-in. Optionally, user can be put in a quarantine group where (s)he gets limited access to internal network resources.

In this article, we will try to use EPA scan as an initial check in a nFactor or multi factor authentication. As an example, we will try to implement the following logic.


User connects to Netscaler
EPA Scan for User browser version
EPA scan success
Radius or OTP Authentication
EPA scan Failure
LDAP Or AD Authentication

User connects to NetScaler Gateway Virtual IP. An EPA scan is initiated. If EPA scan is successful user is rendered with login page with username and password fields for RADIUS or OTP based authentication. Else user is rendered with a login page, but this time will be authenticated using LDAP or AD (Active Directory) based authentication. Based on the success or failure of user provided credentials, user is provided access.

To implement this logic, post EPA:

1. if scan is successful user is placed or tagged to a default user group.
2. If scan was a failure, then user is placed or tagged to a quarantine group.
3. The next method of authentication (RADIUS or LDAP) is chosen based on user group membership as determined in the first two steps.

Pre-requisites

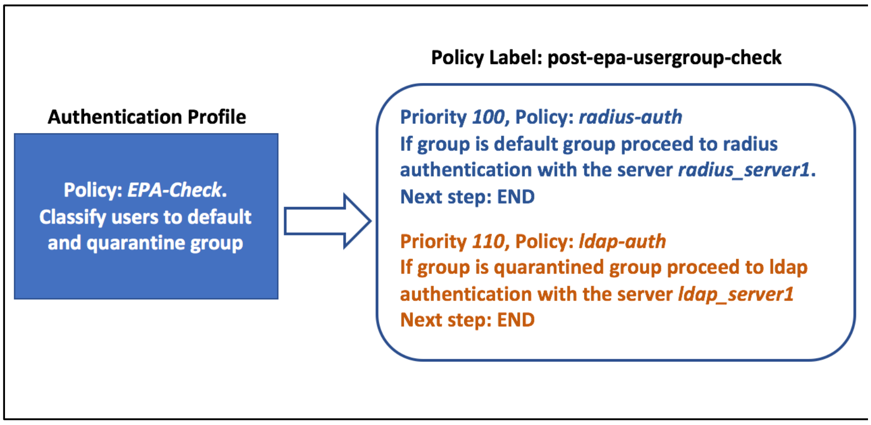
It is assumed that following configuration are in place.

- VPN Vserver/Gateway and Authentication Vserver configurations
- AAA user groups (for default & quarantined user groups) and associated policies
- LDAP and Radius server configurations and associated policies.

As part of this guide, the required policies and policy label configurations will be shown and associate it to an authentication profile.

Instructions

Below graph shows mapping of policies and policy label. We will use this approach for configuring, but from right to left.



Authentication Profile

Policy: *EPA-Check*. Classify users to default and quarantine group

Policy Label: post-epa-usergroup-check

Priority *100*, Policy: *radius-auth*
If group is default group proceed to radius authentication with the server *radius_server1*.
Next step: END

Priority *110*, Policy: *ldap-auth*
If group is quarantined group proceed to ldap authentication with the server *ldap_server1*
Next step: END

Configuration Steps

CLI configurations steps below

1. Configure **ldap-auth** policy to check for ***quarantined_group*** membership and associate it with a LDAP policy which is configured to authenticate with a particular LDAP server.

   Formatted: Font:Bold

   ```
   add authentication Policy ldap-auth -rule "HTTP.REQ.USER.IS_MEMBER_OF(\"quarantined_group\")" -action ldap_server1
   ```

   ldap_server1 is LDAP policy and **ldap-auth** is policy name

2. Configure **radius-auth** policy to check for ***default_group*** membership and associate it with a Radius policy which is configured to authenticate with a particular Radius server.

   Formatted: Font:Bold

   ```
   add authentication Policy radius-auth -rule "HTTP.REQ.USER.IS_MEMBER_OF(\"default_group\")" -action radius_server1
   ```

   radius_server1 is Radius Policy and **radius-auth** is policy name

3. Configure Policy label ***post-epa-usergroup-check***, with Loginschema to capture single factor username and password.

   ```
   add authentication policylabel post-epa-usergroup-check -loginSchema lschema_single_factor_deviceid
   ```

   Note: Replace with the schema you need, in case you do not want to use inbuilt schema **lschema_single_factor_deviceid**

4. Associate policies configured in step 1 and 2 with policy label configured in step 3.

   ```
   bind authentication policylabel post-epa-usergroup-check -policyName radius-auth -priority 100 -gotoPriorityExpression END
   ```

   ```
   bind authentication policylabel post-epa-usergroup-check -policyName ldap-auth -priority 110 -gotoPriorityExpression END
   ```

   Here END indicates end of authentication mechanism for that leg.

5. Create an action to perform EPA scan and associate it with an EPA scan policy

   ```
   add authentication epaAction EPA-client-scan -csecexpr "sys.client_expr(\"app_0_MAC-BROWSER_1001_VERSION_<=_10.0.3\")||sys.client_expr(\"os_0_win7_sp_1\")" -defaultEPAGroup default_group -quarantineGroup quarantined_group
   ```

Just as an example, the above expression scans if MAC OS users have browser version less than 10.0.3 or if Windows 7 users have Service pack 1 installed. ***default_group*** and ***quarantined_group*** are pre-configured user groups

add authentication Policy EPA-check -rule true -action EPA-client-scan

6. Bringing it all together, associate EPA scan policy to AAA vserver with next step pointing to policy label **post-epa-usergroup-check** to perform next step in authentication

   bind authentication vserver MFA_AAA_vserver -policy EPA-check -priority 100 -nextFactor post-epa-usergroup-check -gotoPriorityExpression NEXT

Additional Resources

Nfactor concepts: https://support.citrix.com/article/CTX222713
LDAP Authentication: https://support.citrix.com/article/CTX108876