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

Objective

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

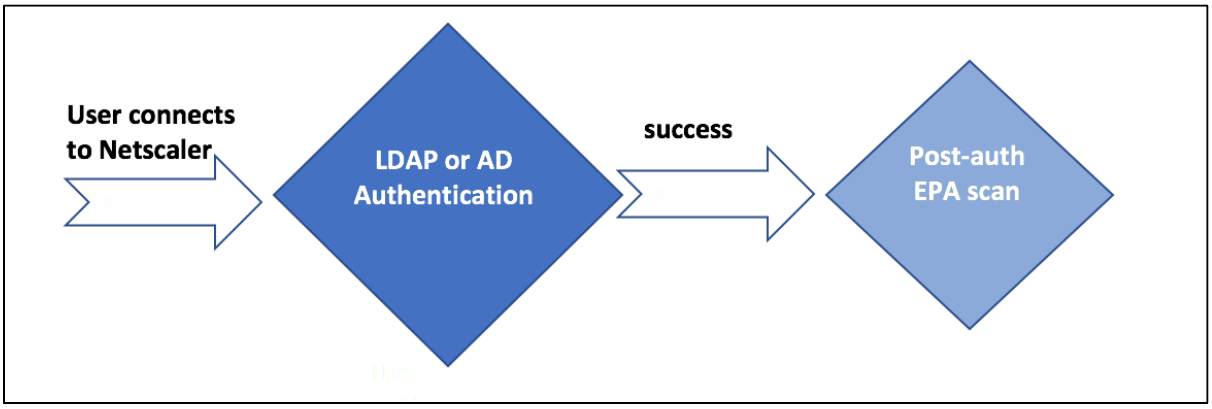
Introduction

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.

Previously post-EPA was configured as part of session policy. Now it can be linked to nfactor providing more flexibility, as to when it can be performed.

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



User tries to connect to NetScaler Gateway Virtual IP. A simple login page with username and password field is rendered to user to provide login credentials. With these credentials, LDAP or AD based authentication is performed at the backend. If successful, user is presented with a pop up to authorize EPA scan. Once user authorizes, EPA scan is performed and based on the success or failure of user client settings, s(he) is provided access.

Pre-requisites

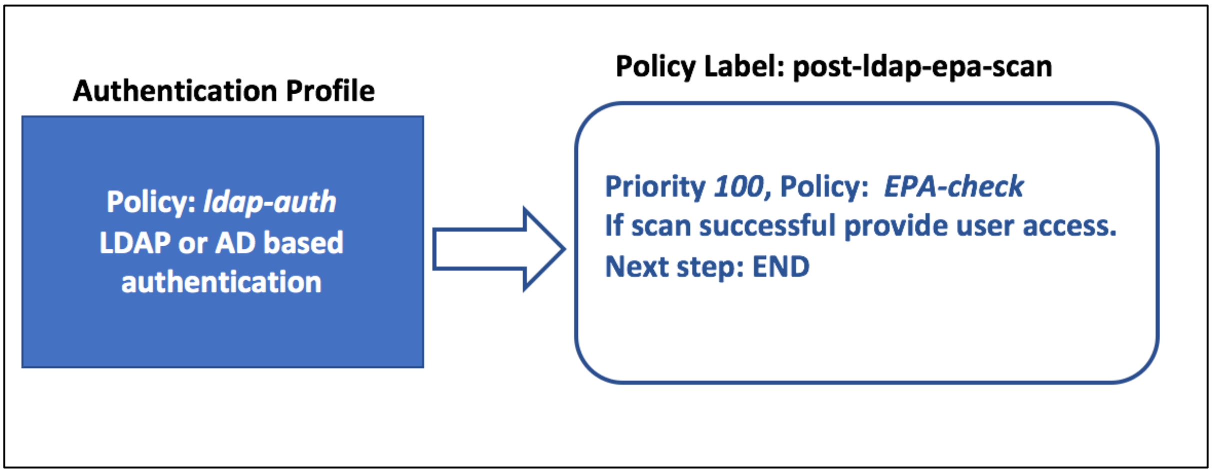
It is assumed that following configuration are in place.

- 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 associate these 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: *ldap-auth*
LDAP or AD based authentication
Policy Label: post-ldap-epa-scan
Priority *100*, Policy: *EPA-check*
If scan successful provide user access.
Next step: END

Configuration Steps

CLI configurations steps below

1. 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\")"
```

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.

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

2. Configure Policy label ***post-ldap-epa-scan***, which will host the policy for EPA scan.

   add authentication policylabel post-ldap-epa-scan -loginSchema LSCHEMA_INT

   Note: **LSCHEMA_INT** is inbuilt schema with no schema(noschema), meaning no additional webpage is presented to user at this step

3. Associate policy configured in step 1 with policy label configured in step 2.

   bind authentication policylabel post-ldap-epa-scan -policyName EPA-check -priority 100 -gotoPriorityExpression END

   Here END indicates end of authentication mechanism.

4. Configure **ldap-auth** policy to and associate it with a LDAP policy which is configured to authenticate with a particular LDAP server.

   add authentication Policy ldap-auth -rule true -action ldap_server1

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

5. Bringing it all together, associate **ldap-auth** policy to AAA vserver with next step pointing to policy label **post-ldap-epa-scan** to perform EPA scan

   bind authentication vserver MFA_AAA_vserver -policy ldap-auth -priority 100 -nextFactor post-ldap-epa-scan -gotoPriorityExpression NEXT

Note

Pre-auth EPA scan is always performed as the first step in nfactor authentication and post-auth EPA scan is always performed as the last step in nfactor authentication. EPA scans cannot be performed in between a nfactor authentication.

Additional Resources

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