SURFsecureID i.c.m. Azure Conditional Access Rules

configuratie en bevindingen

Version 1.0 (08-03-2018)
Peter Ruiter (2AT)

Inhoudsopgave

Inleiding

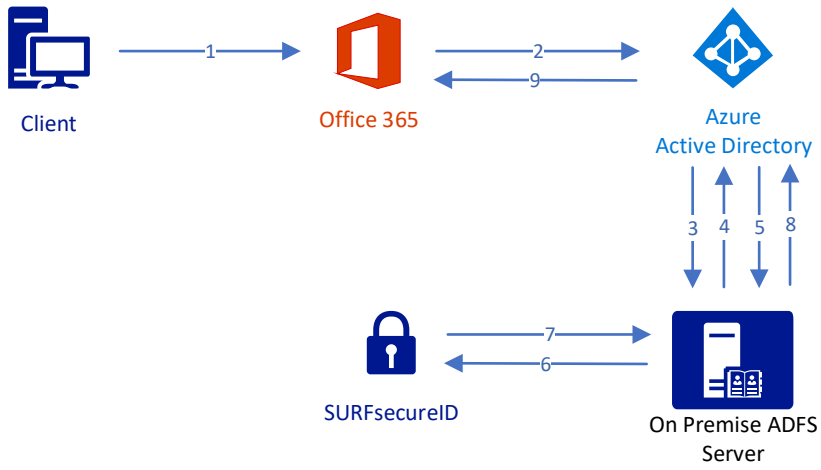
De onderzoeksvraag voor het project is als volgt gedefinieerd:

- Kunnen we SURFsecureID als MFA methode gebruiken op de on-premise ADFS terwijl we hierbij de Conditional Access rules in Azure AD hanteren.

In deze opstelling wordt dus eerst een normaal authenticatieverzoek naar de ADFS server gestuurd. Daar logt de user in zonder MFA. Vervolgens komt de user terug bij Azure AD alwaar middels het Azure AD Conditional Access beleid in de Azure Portal eventueel wordt bepaald of MFA nodig is.

Indien dit het geval is wordt de user wederom naar de On-Premise ADFS server gestuurd waar de gebruiker moet kunnen kiezen uit de verschillende MFA methodes die daar ter beschikking worden gesteld.

Indien dat gelukt is wordt de user weer naar AzureAD gestuurd waar de geslaagde MFA wordt ontvangen en de user verder mag naar de dienst / service.



versimpelde weergave communicatiestappen

Requirements

Voor deze onderzoeksvraag gebruiken we de referentie-omgeving van het Hartingcollege. Deze omgeving bestaat uit een On-Premise ADFS server welke middels AzureAD Connect wordt gesynchroniseerd naar Azure. We gaan in de rest van het document uit van een standaard setup zonder verdere afwijkende instellingen.

Om gebruik te maken van Azure Conditional Access Rules is er een Azure premium P1 of P2 licentie nodig.

Voor deze onderzoeksvraag stellen we op de On-Premise ADFS server geen Access Control Policies in op de Relying Party Trust die eventueel MFA triggeren voordat de Azure AD Conditional Access Rules getriggerd worden. Deze onderzoeksvraag richt zich op het scenario waarbij de regels in Azure AD worden opgesteld.

App met Office 365 account en MFA via On Premises AD FS

Configuratie SURFsecureID

We hebben voor de configuratie van SURFsecureID een pre-compiled versie gebruikt, die hier te vinden is:

https://github.com/SURFnet/ADFS-MFA-SAML2.0-Extension/releases/tag/1.0.1

Het .zip bestand kan worden uitgepakt en vervolgens moet het bestand 'SurfnetMfaPluginConfiguration.json' worden aangepast. Voor de Harting College omgeving hebben we de volgende configuratie gebruikt:

```
{
   "Settings":  {
                "SecondFactorEndpoint":  "https://sa-gw.test.surfconext.nl/second-factor-only/single-sign-on",
                "MinimalLoa":  "http://test.surfconext.nl/assurance/sfo-level2",
                "schacHomeOrganization":  "hartingcollege.nl",
                "ActiveDirectoryName":  "hartingcollege.nl",
                "ActiveDirectoryUserIdAttribute":  "sAMAccountName"
            },
   "ServiceProvider":  {
                    "SigningCertificate":  "signing.hartingcollege.nl.pfx",
                    "EntityId":  "http://adfs.hartingcollege.nl/adfs/services/trust"
                },
   "IdentityProvider":  {
                     "EntityId":  "https://sa-gw.test.surfconext.nl/second-factor-only/metadata",
                     "Certificate":  "sa_test_saml_signing_certificate_pem.crt"
                 }
}
```

Vervolgens dient het 'Install-SurfnetMfaPlugin.ps1' script te worden uitgevoerd. De module zal dan worden geïnstalleerd met de zojuist opgegeven configuratie.

Er zal output op het scherm worden getoond die aan SURFnet moet worden doorgegeven. Dit ziet er als volgt uit:

Geef onderstaande gegevens door aan SURFnet
Issuer: http://adfs.hartingcollege.nl/adfs/services/trust


```
-----BEGIN CERTIFICATE-----
MIIDAzCCAeugAwIBAgIQGaxmfLZl4ZlMYkVEEVdPkjANBgkqhkiG9w0BAQsFADAkMSIwIAYDVQQD
DBlzaWduaW5nLmhhcnRpbmdjb2xsZWdlLm5sMB4XDTE4MDIyNzExMzg1NFoXDTIzMDIyODExMzg1
NFowJDEiMCAGA1UEAwwZc2lnbmluZy5oYXJ0aW5nY29sbGVnZS5ubDCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBALKvZgtLQJTFH2Od0XgHZMzvMopsfcYC/G2ct5i1B5GZuEPNWsoASd9J
iQUoZvMM0IN7wvjlG2tcWZzABSO0xc/lKrJG4DDPRqvzzMlEnWmq78L+WVcMAJqZP7dL7QFB3c8E
dyj6F9Z67mzGDcb4vKY+mClaOEWNmQmlRUvKQyVj5AqsFhmKuySS35brOAkKqNZLeWcaBvMTGoD6
Xpk3R9FobQ9HRBe3o3KebYPu/1E2rb397YiL/i9aO2B/ciDjDtK1svN3FCyc0/cxsOLFq0+8moqI
zJxsk3agLY1o3cKbGwNA/01e4x/GLS1NVhooA4XSlWsB9C1PdQu5gRTsWoUCAwEAAaMxMC8wDgYD
VR0PAQH/BAQDAgeAMB0GA1UdDgQWBBSBbPsjlcAFnN0+u3OnVYgkzvqdOjANBgkqhkiG9w0BAQsF
AAOCAQEAMrbsCkVG7X9sqZvl8vWPo7lgJgofl82f05W3UUBNfMCdgRpAQU+khc7Yevg6ubxtFOMX
a6TRQvAS3Re8VrlbPzNggeYe1fCPH3WZd6sDylSUGO4aIg1gVXiPhJesKfAGAhOiLLlZi0DpsZmw
Z9IGfJxl1c9iQhiO5l+Z4y4ZwntKIIPmkpMkLalgtEoimgc+UXF1Q5aDx9nVFtn4gj2EutX7YocO
3RnoCzFDMwZk8C4CjID4kx4urZDLEU56K0C5QOPUeqhKJdj8D/rfNQ/0gpGwTNTEmTwQD45DjYuS
CPB1RTXdfsYhjPx6FH1YexrUJoprdevu2flEGjEu09lDVA==
-----END CERTIFICATE-----
```

Instellen SupportsMFA parameter

De oplossing van deze onderzoeksvraag ligt bij de *SupportsMFA* parameter binnen de MSOLDomainFederationSettings configuratie. Door deze op **True** te zetten vertellen we Azure AD (AAD) dat het een federated domain is welke een on-premise MFA mogelijkheid heeft. Zodra er een behoefte bestaat om een second factor authenticatie te doen stuurt Azure hierdoor een request naar de STS IDP (bijv. ADFS) in plaats van zijn eigen Azure Cloud MFA te triggeren.

Om deze parameter in te stellen dien je te verbinden met de AAD tenant. Let op dat de commandlets hieronder niet in de nieuwe PowerShell module (AzureAD) voor AAD zitten. Op het moment van schrijven zijn deze enkel uit te voeren middels de oudere AAD module.

Open een PowerShell scherm als admin en voer het volgende commando uit:
Connect-MSOLService

Voer de logingegevens van de tenantadministrator in om te verbinden.

Voer verbolgens de volgende commando's in:

```
$dom = "hartingcollege.nl"
$slo = https://adfs.hartingcollege.nl/adfs/ls/
$idp = http://adfs.hartingcollege.nl/adfs/services/trust
$sso = https://adfs.hartingcollege.nl/adfs/ls/
$crt =
"MIIC6DCCAdCgAwIBAgIQO+pBPv/5hphJGrsG2mR3dzANBgkqhkiG9w0BAQsFADAwMS4wLA
YDVQQDEyVBREZTIFNpZ25pbmcgLSBhZGZzLmhhcnRpbmdjb2xsZWdlLm5sMB4XDTE3MDcw
NDEwMDA0NFoXDTIyMDcwMzEwMDA0NFowMDEuMCwGA1UEAxMlQURGUyBTaWduaW5nIC0g
YWRmcy5oYXJ0aW5nY29sbGVnZS5ubDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQo
CggEBAM+NoZ4mk887ocwuf25GUtoDMpkqvnqz5aq+BfV/+2DoEwZ6N+zUoLyzirQAok0tnx3wE
Y/1MNz0QdDtQYZCP7dn68+/Qgy25T+Lljql/O47qWqxLU9h/pL++kb7h0jMgqmzWz5prFvHQQgp1
mPp1C++0+qY8LzPN70k749VRBDuvr3IAShNWgq8AHmvUP6uZnBFJ0hlhSsRhG3sbpYHsSW6O
FPYDvn2in+kO6r6zUHXGd0WWdQkmahl2l/oA6EAAjuZ/ROkFJJ2zyDK+uLDHezB/QZv29y0q7GO
ZLCpC76nl0HuFUqUq+Y4QT4G3XG4qeTIEUUDtKYa369LiOrn9rECAwEAATANBgkqhkiG9w0BA
QsFAAOCAQEAftNvegr05K3j6ypnmx9DB/ZiE8ddH9L96XwQUOl+qKdXhwwDJ0NglPnyk+TMmd
TZUKAOK90K1dYaJqZkuZGv++gqv4Gz5S3LCaTjNfe87ivVZjbFZ9/Cxngt69DMV9Eh7TD6mS2E9
DiFM8BJt1m9SXmV9Yn5QWpeY+6shj7pAvdVufrPOPjoHepsYK1XbHsH/sAszFcA7m1ijAYsWHP
xbOYQtPwcXf2F5fo2yRHUZDTHxKTSjySLhGBp+6pH2116R8+ECvIDf9E6yKPZI7arjzBfNkt+nvbx
o33tudL7oy6a7bQKh/AoJA1IVSIkfmEQc+QhehWw9jXjvOllYHXYSQ==="

Set-MsolDomainAuthentication –DomainName $dom -Authentication Managed
Set-MsolDomainAuthentication –DomainName $dom -FederationBrandName $dom -
Authentication Federated -PassiveLogOnUri $sso -SigningCertificate $crt -IssuerUri $idp -
LogOffUri $slo -PreferredAuthenticationProtocol WsFed

Set-MsolDomainFederationSettings -domain hartingcollege.nl -SupportsMFA $true
```

Opmerking: Voor de werking maakt het niet uit of WSFed of Samlp wordt gebruikt. In bovenstaand commando zijn de paden en het signing certificaat uiteraard voor het hartingcollege. Let op dat bij het wijzigen van deze setting het 15-30 minuten kan duren voordat het effect zichtbaar is.

Inrichten Conditional Access Rules op Azure

Stel de gewenste Azure Conditional Acces Rules (Voorwaardelijke toegang) in binnen de AAD omgeving op Azure. Porteer eventuele regels die je eerder had staan op je On-Premise ADFS server.

Om de opstelling te testen hebben we voor één van onze testusers een aparte regel gemaakt die er uit ziet als volgt:

Naam: MFA – Only for Medewerker06

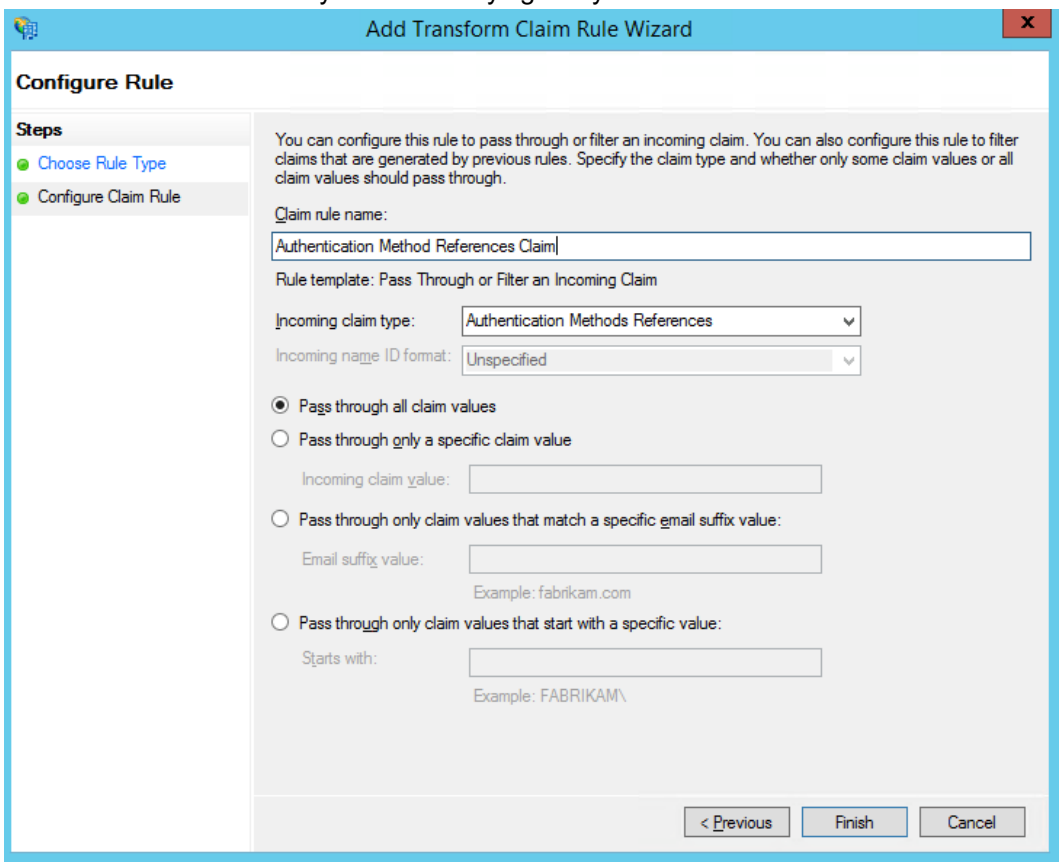
Toewijzingen
Gebruikers en groepen -> Gebruikers en groepen selecteren -> Gebruikers en groepen -> medewerker06@hartingcollege.nl
Cloud-apps -> Alle cloud-apps
Voorwaarden -> Locaties -> Elke locatie

Besturingselementen voor toegang
Verlenen -> Toegang verlenen -> Meervoudige verificatie vereisen

Middels bovenstaande regels wordt voor medewerker06@hartingcollege altijd extra MFA vereist.

ADFS claims configureren

We moeten zorgen dat de claim **authnmethodsreferences** wordt doorgezonden. Deze claim wordt gegenereerd wanneer ADFS succesvol MFA doorloopt. Het is hoe ADFS aan Azure AD vertelt dat het MFA heeft gedaan voor de user. Maak hiervoor een PassThrough Transform Claim Rule aan op de Microsoft Office 365 Identity Platform Relying Party Trust.



Uitschakelen ADFS MFA regels

Verwijder de Access Control Policies op de ADFS server welke voor deze Relying Party trust MFA zouden kunnen triggeren.

Open hiervoor een PowerShell venster als Administrator op de ADFS server en voer het volgende commando uit:

Set-AdfsRelyingPartyTrust -TargetName "Microsoft Office 365 Identity Platform" -AdditionalAuthenticationRules $null

Opmerking: Indien er regels op de ADFS server blijven staan die MFA triggeren zal ADFS direct een claim meesturen die aangeeft dat MFA is gedaan, maar zal Azure AD vervolgens alsnog zijn beleidsregels checken. Indien daar enkel staat dat MFA noodzakelijk is zal Azure AD zien aan de

claim en niet nogmaals MFA vragen. Indien in Azure AD bijvoorbeeld staat dat er een specifieke MFA methode gebruikt moet worden die je niet hebt gebruikt bij de MFA getriggered door ADFS, dan zal Azure AD dus nogmaals afdwingen om aan zijn beleidsregels te voldoen.

Conclusie

We hebben succesvol de onderzoeksvraag kunnen beantwoorden. We zien het volgende nu gebeuren in de praktijk:

De gebruiker probeert zich aan te melden bij een Azure AD toepassing. Aangezien hun domein gefedereerd is, worden ze omgeleid naar de On-Premise ADFS server om zich aan te melden.

De gebruiker zal een standaard gebruikersnaam/wachtwoord authenticatie uitvoeren.

Eenmaal succesvol geauthenticeerd, zullen ze teruggestuurd worden naar Azure AD met een SAML token. Nu is het het moment waarop Azure AD de CA beleidsregels zal beoordelen en bepaalt of de gebruiker MFA nodig heeft of niet.

Als ze dat wel doen, genereert Azure AD daadwerkelijk een nieuw ADFS login-verzoek, dit keer met de specifieke vermelding via de **wauth** parameter om **multipleauthn** te gebruiken. Dit zal de ADFS effectief vertellen om MFA uit te voeren met behulp van de geconfigureerde providers.

Zodra de gebruiker met succes MFA heeft voltooid, zullen ze teruggaan naar Azure AD met deze nieuwe SAML token dat een claim bevat die Azure AD vertelt dat MFA nu is uitgevoerd en deze laat de gebruiker vervolgens door.