Sécuriser RDP avec Azure MFA via l'extension NPS : guide complet

L'extension NPS (Network Policy Server) pour Azure MFA ajoute une authentification multifacteur push/TOTP sur les connexions RDP existantes, sans modifier l'infrastructure cliente. Déployée en 2 heures sur un serveur NPS Windows, elle transforme un accès RDP vulnérable en flux sécurisé conforme aux exigences MFA modernes.

Le protocole **RDP (Remote Desktop Protocol)** est l'une des cibles favorites des attaquants en 2026. Plus de 4 millions de ports RDP sont exposés directement sur Internet selon Shodan, et les attaques par bruteforce sur RDP représentent régulièrement 30 à 40 % des vecteurs d'entrée dans les incidents ransomware selon le Panorama de la cybermenace ANSSI. La solution la plus accessible pour sécuriser immédiatement ces accès sans refonte de l'infrastructure est l'**extension NPS pour Azure MFA** (Network Policy Server). Cette extension, déployée sur un serveur Windows NPS existant ou à créer, s'intercale dans le flux d'authentification RADIUS de vos accès RDP et exige un second facteur Azure MFA (push notification, TOTP, appel téléphonique) après validation du mot de passe Active Directory. Résultat : **azure MFA RDP NPS extension** sécurise tous vos accès RDP sans modifier les postes clients, sans déployer de VPN supplémentaire, sans changer l'infrastructure AD — en deux heures de déploiement. Ce guide complet couvre les prérequis de licences et d'architecture, l'installation pas à pas de l'extension via PowerShell, la configuration du client RADIUS dans NPS, les politiques de connexion (Connection Request Policy et Network Policy), la procédure de test, le dépannage avec les logs NPS et Azure, et les alternatives selon les cas.

À RETENIR

À retenir

Licences requises : Azure MFA nécessite Azure AD P1 (inclus dans Microsoft 365 Business Premium, E3, E5) ou des licences MFA Azure standalone.

NPS Windows requis : le rôle NPS (Network Policy Server) doit être installé sur un serveur Windows Server 2019/2022 joint au domaine AD.

RADIUS client : la Passerelle Bureau à distance (RD Gateway) ou votre VPN doit être configurée comme client RADIUS pointant vers le NPS.

Pas de modification client : les utilisateurs se connectent comme d'habitude — le second facteur est demandé par Azure MFA après le mot de passe AD.

Logs de dépannage : les logs de l'extension NPS sont dans `c:\Windows\Logs\Microsoft\AzureMfa\` — premier réflexe en cas de problème.

Pourquoi MFA sur RDP est non-négociable en 2026 ?

La réponse courte : parce qu'un mot de passe seul sur RDP ne protège plus rien. Les attaques par credential stuffing (utilisation de bases de données de mots de passe compromis), bruteforce et password spraying contre les ports RDP exposés sont entièrement automatisées en 2026. Des services comme **xDedic** ou **Genesis Market** (avant leur démantèlement) vendaient des accès RDP compromis à quelques dollars — le ROI pour les attaquants est excellent.

L'ANSSI dans son Panorama de la cybermenace 2025 identifie les accès RDP exposés ou mal sécurisés comme l'un des principaux vecteurs d'entrée dans les incidents ransomware sur les

organisations françaises. La recommandation est unanime : **MFA obligatoire sur tous les accès distants**, RDP inclus.

L'extension NPS pour Azure MFA est la solution la plus rapide à déployer pour les organisations qui utilisent déjà Microsoft 365 ou Azure AD — car les licences Azure MFA sont souvent déjà incluses dans leurs abonnements existants, sans coût supplémentaire. C'est aussi la solution qui perturbe le moins les utilisateurs finaux : ils continuent d'utiliser leur client RDP habituel, et reçoivent juste une notification push sur leur téléphone après la saisie du mot de passe.

Architecture : comment fonctionne NPS + extension Azure MFA

Comprendre le flux d'authentification est essentiel avant de configurer quoi que ce soit. Voici la séquence complète :

L'utilisateur lance une connexion RDP vers le serveur cible (via RD Gateway ou directement)

La **Passerelle Bureau à distance (RD Gateway)** intercepte la connexion et envoie une requête RADIUS d'authentification au serveur NPS

Le serveur **NPS** valide le mot de passe de l'utilisateur contre Active Directory

Si le mot de passe est valide, l'**extension NPS Azure MFA** intercepte la requête et contacte Azure MFA (cloud Microsft) via HTTPS

Azure MFA envoie une notification push à l'application Microsoft Authenticator sur le téléphone de l'utilisateur

L'utilisateur approuve la notification (ou entre son TOTP)

Azure MFA retourne un succès à l'extension NPS

NPS retourne un succès à RD Gateway

La connexion RDP est établie

Ce flux montre clairement que **l'extension NPS nécessite une connexion HTTPS sortante** vers les endpoints Azure MFA (login.microsoftonline.com, aadcdn.msftauth.net). Si votre serveur NPS est dans un réseau très fermé, vérifiez que ces endpoints sont accessibles avant de commencer.

Environnement de test : Windows Server 2022 (NPS + RD Gateway), Azure AD tenant M365 Business Premium, 15 utilisateurs, Microsoft Authenticator sur iOS et Android. Déploiement réalisé en 90 minutes.

Comparatif des méthodes de second facteur Azure MFA

Avant de déployer, choisissez la méthode MFA adaptée à votre organisation. Chaque méthode présente des compromis sécurité/friction utilisateur différents :

Méthode MFA	Niveau de sécurité	Friction utilisateur	Prérequis	Résistance au phishing
Push notification (Authenticator)	Élevé	Faible (1 tap)	Smartphone + app Microsoft Authenticator	Partielle (vulnérable MFA fatigue)
TOTP (code 6 chiffres)	Élevé	Moyenne (saisir le code)	Smartphone ou clé physique	Partielle
Appel téléphonique	Moyen	Élevée (décrocher)	Téléphone fixe ou mobile	Faible (SIM swapping possible)
SMS (code OTP)	Faible	Moyenne	Mobile avec réseau SMS	Très faible (interception SS7)
Clé FIDO2/WebAuthn	Très élevé	Très faible (touch)	Clé physique (YubiKey, Titan)	Totale (non supporté par ext. NPS)

La méthode recommandée pour la majorité des organisations est la **push notification via Microsoft Authenticator** — le meilleur équilibre sécurité/adoption. Pour les utilisateurs exposés à des tentatives de phishing ciblées, activez le **Number Matching** dans Azure AD (l'utilisateur doit confirmer un nombre affiché sur l'écran de connexion, empêchant l'approbation aveugle) pour résoudre le problème de MFA fatigue.

Prérequis : licences, NPS et tenant Azure

Avant de lancer l'installation, vérifiez chaque prérequis de cette liste — une erreur ici coûte des heures de dépannage plus tard.

Licences : Azure MFA nécessite Azure AD Premium P1 au minimum. Ce niveau est inclus dans :

Microsoft 365 Business Premium

Microsoft 365 E3 / E5

Enterprise Mobility + Security (EMS) E3/E5

Azure AD Premium P1 standalone (6 $/user/mois)

Le plan Microsoft 365 Business Basic ou Standard n'inclut pas Azure AD P1 — vérifiez votre plan dans le portail admin M365 → Licences.

Serveur NPS : Windows Server 2019 ou 2022, joint au domaine AD. Le rôle NPS peut coexister sur un serveur existant (contrôleur de domaine secondaire, serveur d'applications) ou sur un serveur dédié. Évitez d'installer NPS sur un contrôleur de domaine primaire en production — privilégiez un serveur membre.

Connectivité : le serveur NPS doit pouvoir joindre en HTTPS sortant :

`login.microsoftonline.com` (port 443)

`*.aadcdn.msftauth.net` (port 443)

`adnotifications.windowsazure.com` (port 443)

```
 # Vérifier la connectivité depuis le serveur NPS
Test-NetConnection -ComputerName login.microsoftonline.com -Port 443
Test-NetConnection -ComputerName adnotifications.windowsazure.com -Port 443
# TcpTestSucceeded : True pour les deux = OK
```

Installer le rôle NPS sur Windows Server

Si NPS n'est pas encore installé sur votre serveur, voici l'installation via PowerShell :

```
 # Installer le rôle NPS et les outils d'administration
Install-WindowsFeature -Name NPAS -IncludeManagementTools

# Vérifier l'installation
Get-WindowsFeature -Name NPAS
# DisplayName : Services de stratégie et d'accès réseau
# Installed : True

# Démarrer et configurer le service NPS au démarrage automatique
Set-Service -Name IAS -StartupType Automatic
Start-Service -Name IAS
```

Installer l'extension NPS pour Azure MFA

L'extension est disponible sur le Microsoft Learn et s'installe via un package MSI ou directement en PowerShell. Voici la procédure complète :

```
 # Étape 1 : Télécharger l'extension NPS depuis le Centre de téléchargement Microsoft
# URL : https://aka.ms/npsmfa (redirige vers le dernier MSI)

# Étape 2 : Installer l'extension (exécuter en tant qu'administrateur local)
# Double-cliquer sur le MSI ou via PowerShell :
Start-Process -FilePath "NPS extension for Azure MFA.msi" -Wait

# Étape 3 : Exécuter le script de configuration PowerShell
# Le script est installé dans C:\Program Files\Microsoft\AzureMfa\Configcd "C:\Program Files\Micr

# Récupérer votre Tenant ID Azure AD
$TenantId = (Get-AzureADTenantDetail).ObjectId  # nécessite AzureAD module
# Ou depuis le portail Azure AD -> Vue d'ensemble -> ID du répertoire

# Exécuter le script de configuration
.\AzureMfaNpsExtnConfigSetup.ps1 -tenantId "VOTRE_TENANT_ID"
```

Le script de configuration effectue plusieurs opérations automatiquement :

Crée un principal de service dans Azure AD avec les permissions MFA requises

Génère et installe un certificat auto-signé pour l'authentification entre l'extension et Azure

Configure le registre Windows avec les paramètres de l'extension

Redémarre le service NPS

```
 # Vérifier que le certificat a bien été créé
Get-ChildItem Cert:\LocalMachine\My | Where-Object Subject -like "*Microsoft Azure MFA*"
# CN=Microsoft Azure MFA NDESCONNECTOR — doit être présent

# Vérifier le service NPS après configuration
Get-Service IAS
# Status : Running
```

Configurer le client RADIUS dans NPS

Le serveur NPS doit connaître les équipements qui lui enverront des requêtes RADIUS (RD Gateway, VPN, switch 802.1X). Ces équipements sont configurés comme "clients RADIUS" dans la console NPS.

```
 # Ouvrir la console NPS
nps.msc

# Ou ajouter un client RADIUS via PowerShell
New-NpsRadiusClient -Address "192.168.1.10" `
    -Name "RD-Gateway-Prod" `
    -SharedSecret "SECRET_RADIUS_FORT_AU_MOINS_22_CHARS" `
    -AuthAttributeRequired $false

# Vérifier les clients RADIUS configurés
Get-NpsRadiusClient
```

Le **shared secret RADIUS** est le secret partagé entre le client RADIUS (RD Gateway) et le serveur NPS. Il doit être identique des deux côtés et d'une longueur minimale de 22 caractères. Générez-le avec :

```
# Générer un secret RADIUS fort
[System.Web.Security.Membership]::GeneratePassword(32, 8)
# Résultat exemple : K7#mN2@pQ8!rX5&wB3$vY6^jL4*hZ1%d
```

Connection Request Policy et Network Policy

NPS utilise deux types de politiques pour décider si une connexion est autorisée :

Connection Request Policy (Stratégie de demande de connexion) : détermine si le serveur NPS traite lui-même la demande ou la redirige vers un autre serveur RADIUS. Pour notre cas, créez une politique qui accepte les demandes entrantes depuis vos clients RADIUS (RD Gateway).

```
# Créer une Connection Request Policy via PowerShell
New-NpsConnectionRequestPolicy `
    -Name "Politique-RDP-Azure-MFA" `
    -Condition "CALLING-STATION-ID Matches .*" `
    -PolicyOrder 1 `
    -AuthenticationProviders @{Id="Windows";Type="Windows"} `
    -Enabled $true
```

Network Policy (Stratégie réseau) : détermine quels utilisateurs sont autorisés et dans quelles conditions. Configurez une politique qui autorise les membres du groupe de sécurité AD dédié aux accès RDP :

```
# Créer un groupe AD dédié aux utilisateurs RDP avec MFA (si pas déjà existant)
New-ADGroup -Name "GRP-RDP-MFA-Autorise" -GroupScope Global -GroupCategory Security

# Ajouter des utilisateurs au groupe
Add-ADGroupMember -Identity "GRP-RDP-MFA-Autorise" -Members "utilisateur1","utilisateur2"
```

Dans la console NPS → Network Policies, créez une nouvelle politique avec :

Condition : **Windows Groups** = `GRP-RDP-MFA-Autorise`

Condition : **Client Friendly Name** = `RD-Gateway-Prod`

Accès accordé (Access Granted)

Méthode d'authentification : Microsoft Encrypted Authentication (MS-CHAPv2) ou EAP/PEAP selon votre config

Configurer la Passerelle Bureau à distance (RD Gateway)

La RD Gateway doit pointer vers le NPS comme serveur RADIUS central pour l'authentification :

```
 # Sur le serveur RD Gateway — configurer le client RADIUS
# (Gestionnaire de Passerelle Bureau à distance → Propriétés → Magasin de demandes CAP)

# Ou via PowerShell (module RemoteDesktop)
Import-Module RemoteDesktop

# Configurer le serveur NPS comme backend d'authentification
Set-RDGatewayConfiguration -CentralRequestPolicy CentralNAP `
    -RadiusServerName "192.168.1.20" `      # IP du serveur NPS
    -RadiusServerPort 1812 `
    -RadiusSharedSecret "SECRET_RADIUS_FORT_AU_MOINS_22_CHARS"
```

Tester l'authentification RDP avec MFA

Avant de déployer en production, testez avec un compte pilote :

```
 # Test de la connexion RADIUS depuis le serveur NPS
# (outil natif radclient ou via la console NPS → Test des clients RADIUS)

# Vérifier les logs NPS en temps réel
Get-WinEvent -LogName "Security" -MaxEvents 50 |
    Where-Object {$_.Id -in (6272, 6273, 6274)} |
    Select-Object TimeCreated, Id, Message |
    Format-List

# Events clés NPS :
# 6272 : Accès réseau accordé (succès MFA)
# 6273 : Accès réseau refusé (échec password ou MFA)
# 6274 : Demande de connexion ignorée
```

Procédure de test manuelle :

Connectez un client RDP vers votre serveur via RD Gateway

Entrez vos identifiants AD (nom d'utilisateur + mot de passe)

Attendez 10–30 secondes — la notification push apparaît sur le téléphone

Approuvez la notification dans Microsoft Authenticator

La connexion RDP s'établit

Si la connexion échoue à l'étape 3 (timeout sans notification), c'est un problème de connectivité entre le serveur NPS et Azure MFA. Vérifiez les logs de l'extension.

Dépannage : logs NPS et extension Azure MFA

Les logs sont répartis entre deux emplacements. Premier réflexe en cas de problème :

```
 # Logs de l'extension NPS Azure MFA
# Emplacement : C:\Windows\Logs\Microsoft\AzureMfaGet-Content "C:\Windows\Logs\Microsoft\AzureMfa

# Logs du service NPS (Observateur d'événements)
Get-WinEvent -LogName "System" -ProviderName "IAS" -MaxEvents 20 |
    Select-Object TimeCreated, Id, LevelDisplayName, Message |
    Format-List

# Messages d'erreur fréquents et leur signification :
# "Access-Reject due to failed MFA" : l'utilisateur a refusé ou ignoré la notification
# "Error connecting to Azure MFA" : problème réseau vers Azure (vérifier le firewall)
# "User not found in Azure AD" : l'UPN Azure AD ne correspond pas au compte AD local
# "Certificate expired" : le certificat auto-signé de l'extension a expiré (renouveler)
```

Problème fréquent : **le compte AD local et l'UPN Azure AD ne correspondent pas**. Si l'utilisateur a le login AD `jdupont` mais l'email Azure AD `jean.dupont@entreprise.fr`, l'extension NPS ne peut pas corréler les deux. La solution est de s'assurer que l'attribut `userPrincipalName` dans AD correspond à l'email Azure AD, et que la synchronisation Azure AD Connect est active.

```
 # Vérifier l'UPN d'un utilisateur en AD
Get-ADUser -Identity "jdupont" -Properties UserPrincipalName |
    Select-Object Name, UserPrincipalName, SamAccountName
# UserPrincipalName doit correspondre à l'email Azure AD

# Si discordance — mettre à jour l'UPN
Set-ADUser -Identity "jdupont" -UserPrincipalName "jean.dupont@entreprise.fr"
```

Pour les organisations qui gèrent déjà Microsoft 365 et Entra ID, notre article sur [la sécurisation Entra ID avec Conditional Access et MFA] complète ce guide avec les politiques d'accès conditionnel et notre guide sur [la sécurisation des accès Microsoft 365] couvre les autres vecteurs d'attaque M365. Pour les aspects AD plus larges, notre [service de pentest Active Directory] permet d'identifier d'autres failles avant les attaquants.

Renouveler le certificat de l'extension NPS

Le certificat auto-signé généré lors de l'installation expire après 1 an. Après expiration, l'extension cesse de fonctionner silencieusement — les utilisateurs reçoivent une erreur d'authentification sans message explicite côté client. Planifiez le renouvellement :

```
 # Vérifier la date d'expiration du certificat
Get-ChildItem Cert:\LocalMachine\My |
    Where-Object Subject -like "*Microsoft Azure MFA*" |
    Select-Object Subject, NotBefore, NotAfter, Thumbprint

# Renouveler le certificat — réexécuter le script de configuration
cd "C:\Program Files\Microsoft\AzureMfa\Config"
.\AzureMfaNpsExtnConfigSetup.ps1 -tenantId "VOTRE_TENANT_ID"
# Le script génère un nouveau certificat et renouvelle l'inscription Azure AD
```

Créez une tâche planifiée pour recevoir une alerte 30 jours avant l'expiration :

```
 # Tâche planifiée de vérification mensuelle du certificat
$action = New-ScheduledTaskAction -Execute "powershell.exe" -Argument @'
$cert = Get-ChildItem Cert:\LocalMachine\My | Where-Object Subject -like "*Microsoft Azure MFA*"
$daysLeft = ($cert.NotAfter - (Get-Date)).Days
if ($daysLeft -lt 30) {
    Send-MailMessage -To "admin@entreprise.fr" -Subject "Cert NPS MFA expire dans $daysLeft jours
}
'@
$trigger = New-ScheduledTaskTrigger -Weekly -DaysOfWeek Monday -At 9am
Register-ScheduledTask -TaskName "Check-NPS-MFA-Cert" -Action $action -Trigger $trigger -RunLevel
```

Alternatives à l'extension NPS Azure MFA

L'extension NPS est la solution la plus rapide à déployer, mais elle n'est pas adaptée à tous les contextes. Voici les alternatives selon votre situation.

Azure AD Application Proxy : publie des applications internes (incluant les accès RDP via Remote Desktop Web) derrière Azure AD sans ouvrir de ports entrants. Nécessite un connecteur léger installé dans votre réseau interne. Avantage : gestion centralisée dans Azure, Conditional Access natif, pas de NPS. Inconvénient : nécessite Azure AD P1, ne supporte pas le RDP natif (client mstsc.exe) sans configuration supplémentaire — utilise le HTML5 client web.

SSTP VPN avec MFA : déployez un serveur SSTP VPN Windows (rôle RRAS) avec l'extension NPS Azure MFA, et faites passer tous les accès RDP par le VPN. Plus sécurisé (double chiffrement, VPN + RDP TLS), plus complexe à déployer. Pertinent si vous avez déjà une infrastructure RRAS.

Solutions Zero Trust tier : Cloudflare Access avec WARP (voir notre guide sur Cloudflare Zero Trust), Teleport Enterprise, Pangolin — exposent le RDP via un proxy sans jamais ouvrir le port 3389 sur Internet. Solution architecturalement la plus propre mais aussi la plus coûteuse et complexe à maintenir.

Pour des organisations déjà dans l'écosystème Microsoft avec des licences M365 Business Premium, **l'extension NPS reste le meilleur rapport déploiement/sécurité**. Pour une architecture Zero Trust plus complète, notre article sur l'implémentation Zero Trust détaille les options avancées.

Limites de l'extension NPS Azure MFA

Transparence sur ce qui ne fonctionne pas ou mal avec cette solution :

Single Point of Failure : si votre serveur NPS est indisponible (maintenance, panne), *tous* les accès RDP passant par RD Gateway cessent de fonctionner. Déployez au minimum deux serveurs NPS en haute disponibilité avec la même configuration.

Latence ajoutée : l'extension contacte Azure MFA en HTTPS à chaque authentification — si votre connexion Internet est lente ou si Azure a un incident, le délai avant la notification push peut atteindre 10–30 secondes. Préoccupant pour des utilisateurs habitués à des connexions instantanées.

Dépendance Internet : l'extension NPS nécessite une connexion Internet sortante vers Azure. Dans des environnements très sécurisés sans accès Internet (réseaux OT, sites industriels isolés), cette solution est inapplicable.

Méthodes MFA limitées : l'extension NPS ne supporte pas toutes les méthodes Azure MFA. Elle supporte : notification push (recommandé), TOTP Microsoft Authenticator, appel téléphonique, SMS. Elle ne supporte pas WebAuthn/FIDO2 (clés physiques) — pour ces méthodes, utilisez l'Application Proxy ou une solution Zero Trust.

Questions fréquentes

L'extension NPS Azure MFA est-elle gratuite ?

L'extension elle-même est gratuite — téléchargeable sur le Microsoft Download Center sans coût supplémentaire. Ce qui nécessite une licence payante, c'est **Azure MFA** pour chaque utilisateur : la fonctionnalité MFA est incluse dans Azure AD P1 (et donc dans M365 Business Premium, M365 E3/E5). Si vos utilisateurs ont déjà des licences M365 Business Premium ou E3, vous n'avez rien à acheter en plus. Vérifiez vos licences dans le portail admin Microsoft 365 avant de commencer.

L'extension NPS fonctionne-t-elle avec tous les clients RDP ?

Oui — c'est l'un des grands avantages de cette solution. L'authentification MFA est gérée côté serveur (NPS + RD Gateway), pas côté client. Les utilisateurs continuent d'utiliser le client RDP natif Windows (`mstsc.exe`), le client macOS Microsoft Remote Desktop, les apps iOS/Android, ou tout autre client RDP standard. Aucune installation ni configuration côté client n'est nécessaire. Le second facteur arrive sous forme de notification push sur Microsoft Authenticator — que l'application soit déjà installée pour MFA M365 ou non (si non : l'enrollment se fait lors de la première connexion).

Peut-on imposer MFA uniquement pour les connexions RDP depuis l'extérieur ?

Oui, via la **Network Policy NPS**. Configurez deux politiques distinctes : une pour les connexions internes (IP source = plage réseau interne → accès sans MFA ou avec MFA allégé), une pour les connexions externes (IP source = plage publique via RD Gateway → MFA obligatoire). L'alternative plus moderne est d'utiliser les **Conditional Access Policies d'Azure AD** qui offrent une granularité supérieure : MFA selon le pays de connexion, la conformité du device, l'heure de connexion, etc. Ces politiques d'accès conditionnel dans Entra ID sont détaillées dans notre article sur Entra ID et Conditional Access.

Que se passe-t-il si l'utilisateur n'a pas son téléphone ?

Azure MFA propose plusieurs méthodes de secours configurables : (1) **Codes de secours** : chaque utilisateur peut générer 10 codes à usage unique depuis le portail My Security Info — à imprimer et stocker en lieu sûr. (2) **Appel téléphonique** vers un numéro fixe ou de bureau. (3) **TOTP dans un gestionnaire de mots de passe** (si Bitwarden ou Vaultwarden est configuré avec un token TOTP MFA Microsoft). Configurez au minimum deux méthodes de secours par utilisateur lors de l'enrollment initial pour éviter les situations de blocage.

Comment monitorer les échecs MFA et détecter des tentatives d'attaque ?

Dans le portail Azure AD → Protection de l'identité → Rapport d'authentification (Sign-in logs), filtrez sur les applications "NPS Extension" et les statuts "Failure". Un pic d'échecs MFA (notifications push refusées répétitivement par un même compte) peut indiquer une attaque de type MFA fatigue — l'attaquant connaît le mot de passe et spam l'utilisateur de notifications dans l'espoir qu'il approuve par erreur. Azure AD Identity Protection détecte ces patterns et peut bloquer automatiquement les comptes concernés si le niveau de risque est configuré en conséquence. Selon les recommandations du guide Microsoft Learn sur Azure MFA, activez les rapports de fraude pour permettre aux utilisateurs de signaler les notifications non sollicitées.

Votre infrastructure RDP est exposée et vous souhaitez déployer MFA rapidement ? Notre équipe peut déployer l'extension NPS Azure MFA, configurer RD Gateway et Conditional Access en une journée d'intervention. Contactez notre RSSI externalisé.