Intune : configurer le pare-feu Windows Defender via Endpoint Security

Intune Endpoint Security permet de déployer des profils pare-feu Windows Defender sur l'ensemble du parc Windows géré, sans GPO ni serveur on-premise. La gestion centralisée des règles entrantes/sortantes, des profils Domain/Private/Public et du blocage de protocoles dangereux comme LLMNR ou NetBIOS réduit considérablement la surface d'attaque, y compris pour les postes en télétravail.

Configurer l'**Intune pare-feu Windows Defender via Endpoint Security** (intune pare-feu windows defender) est l'une des actions les plus efficaces — et les plus négligées — pour sécuriser un parc de postes Windows géré par Microsoft Endpoint Manager. Contrairement aux règles de pare-feu déployées par GPO, les profils Intune Endpoint Security s'appliquent aussi bien aux machines **Entra ID Joined** (cloud-only) qu'aux machines hybrides — et le résultat est visible en temps réel dans le tableau de bord de conformité. Mieux encore : les règles suivent l'utilisateur où qu'il soit, au bureau ou en télétravail, sans VPN obligatoire. Sur les audits de postes Windows que j'ai réalisés courant 2025, le pare-feu est systématiquement la première ligne mal configurée : règles trop permissives héritées de l'ancienne GPO, LLMNR actif par défaut, NetBIOS non désactivé sur les interfaces WiFi publiques. Ces lacunes sont exploitées en quelques secondes par des outils comme Responder ou Inveigh pour capturer des hashes NTLM sur les réseaux locaux. Ce guide couvre la création des profils, la gestion des trois types de réseaux (Domain, Private, Public), les règles personnalisées, le blocage de protocoles dangereux et la validation via PowerShell.

À RETENIR

À retenir

Endpoint Security > Firewall : nœud recommandé dans Intune pour la gestion des règles pare-feu — distinct des profils Configuration Device, il offre un reporting de conformité dédié et une granularité accrue.

Trois profils réseau : Domain (réseau d'entreprise), Private (réseau domestique), Public (WiFi public) — chacun avec des règles indépendantes ; le profil Public doit être le plus restrictif, bloquant tout le trafic entrant non sollicité.

Bloquer LLMNR et NetBIOS : ces protocoles hérités sont exploités par les attaques NBNS spoofing et Responder — les désactiver réduit immédiatement le risque de capture de hashes NTLM sur les réseaux locaux.

Règles de fusion locale : par défaut, Intune fusionne les règles MDM et les règles locales ; désactiver cette fusion pour un contrôle centralisé strict dans les environnements sensibles ou réglementés.

Test-NetConnection : outil natif Windows pour valider qu'une règle de pare-feu fonctionne après déploiement — plus fiable que les outils tiers sur les machines managées Intune.

Architecture des profils pare-feu dans Intune Endpoint Security

Intune propose deux endroits pour configurer le pare-feu Windows Defender : le nœud **Configuration > Profils > Endpoint Protection** (ancien, en voie de dépréciation) et le nœud **Endpoint Security > Firewall** (recommandé depuis 2022). La différence n'est pas cosmétique : les profils Endpoint Security offrent un reporting de conformité dédié, des alertes sur les non-

conformités, une visibilité par appareil et une granularité accrue sur les règles entrantes et sortantes.

Dans le nœud Endpoint Security > Firewall, deux types de profils sont disponibles et complémentaires :

Windows Firewall : paramètres globaux du pare-feu — activation par profil réseau, comportement par défaut (Allow/Block), journalisation, fusion des règles locales.

Windows Firewall Rules : règles personnalisées entrantes/sortantes définissant application, port, protocole et action pour des flux spécifiques.

La bonne pratique est de créer un profil Windows Firewall pour les paramètres globaux, puis des profils Windows Firewall Rules séparés par catégorie fonctionnelle — règles métier, règles de blocage sécurité, règles de diagnostic IT — pour faciliter la maintenance et le débogage quand une règle pose problème.

Configurer les paramètres globaux par profil réseau

La configuration se fait dans **Endpoint Security > Firewall > Create Policy > Windows 10 and later > Windows Firewall**. Chaque profil réseau (Domain, Private, Public) dispose de paramètres indépendants. Voici la configuration recommandée pour un environnement d'entreprise :

Paramètre	Domain	Private	Public
Firewall enabled	Enabled	Enabled	Enabled
Block all incoming connections	Non	Non	Oui
Disable notifications when blocked	Oui	Non	Oui
Allow unicast responses to multicast	Non	Non	Non
Inbound connections default action	Block	Block	Block
Outbound connections default action	Allow	Allow	Allow
Log dropped packets	Oui	Oui	Oui
Allow Local Firewall Rules	Selon contexte	Selon contexte	Non (strict)

Pourquoi bloquer toutes les connexions entrantes sur le profil Public ? Parce qu'un poste sur un réseau WiFi public (aéroport, hôtel, café) est exposé à d'autres postes non gérés potentiellement malveillants. Le profil Public doit traiter tout voisin réseau comme hostile par défaut. C'est le niveau de protection minimum recommandé par le CIS Benchmark Windows Desktop v3 et par l'ANSSI dans ses recommandations de durcissement des postes Windows.

Pourquoi bloquer LLMNR et NetBIOS en priorité ?

Si vous ne deviez faire qu'une seule chose avec votre profil pare-feu Intune, ce serait de bloquer LLMNR (Link-Local Multicast Name Resolution, UDP 5355) et NetBIOS Name Service (UDP 137, 138). Ces deux protocoles hérités permettent la résolution de noms sans serveur DNS — pratiques dans les années 2000, dangereux en 2026.

L'attaque est simple et documentée depuis des années : un poste Windows ne trouve pas un nom d'hôte via DNS et émet une requête LLMNR ou NetBIOS en broadcast sur le réseau local. N'importe quelle machine peut répondre en se faisant passer pour la cible. L'outil **Responder** — présent dans Kali Linux et utilisé dans des dizaines de red team et de cas réels — exploite exactement ce mécanisme pour capturer des hashes NTLMv2 en quelques secondes. Ces hashes peuvent ensuite être craqués hors-ligne (Hashcat sur un GPU moderne casse du NTLMv2 à des millions de tentatives par seconde) ou utilisés directement en Pass-the-Hash.

Le groupe **Scattered Spider**, responsable de compromissions de grandes entreprises en 2024-2025, a utilisé cette technique combinée au social engineering pour obtenir des accès initiaux sur des réseaux d'entreprise. Désactiver LLMNR et NetBIOS coupe court à ce vecteur à coût quasi nul.

```
 # Désactiver LLMNR via registre (complémentaire à la règle pare-feu)
# Bloquer UDP 5355 côté réseau ET désactiver le service côté OS
Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient" `
    -Name "EnableMulticast" -Value 0 -Type DWord -Force

# Désactiver NetBIOS sur toutes les interfaces réseau actives
$adapters = Get-WmiObject Win32_NetworkAdapterConfiguration | Where-Object { $_.IPEnabled }
foreach ($adapter in $adapters) {
    # Valeur 2 = NetBIOS désactivé (0=via DHCP, 1=activé, 2=désactivé)
    $result = $adapter.SetTcpipNetbios(2)
    $status = if ($result.ReturnValue -eq 0) { "OK" } else { "ERREUR ($($result.ReturnValue))" }
    Write-Host "NetBIOS sur $($adapter.Description): $status"
}

# Vérifier l'état LLMNR
$llmnr = Get-ItemProperty "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient" `
    -Name "EnableMulticast" -ErrorAction SilentlyContinue
Write-Host "LLMNR EnableMulticast: $($llmnr.EnableMulticast)" # 0 = désactivé

# Tester que le port LLMNR est bien inaccessible depuis l'extérieur
Test-NetConnection -ComputerName "127.0.0.1" -Port 5355
# Attendu : TcpTestSucceeded = False
```

Créer des règles de pare-feu personnalisées via Intune

Les règles personnalisées se créent dans **Endpoint Security > Firewall > Create Policy > Windows Firewall Rules**. Chaque règle définit la direction (Inbound/Outbound), l'action (Allow/Block), le protocole, les ports et l'application. Voici un ensemble de règles de sécurité prioritaires à déployer :

Bloquer LLMNR (UDP 5355) — Inbound — Block — Any profile

Bloquer NetBIOS NS (UDP 137) — Inbound — Block — Any profile

Bloquer NetBIOS DGM (UDP 138) — Inbound — Block — Any profile

Bloquer NetBIOS SSN (TCP 139) — Inbound — Block — Public profile (attention : actif en Domain peut bloquer des partages SMB légitimes)

Bloquer WMI entrant depuis réseaux non-Domain (TCP 135) — Inbound — Block — Public profile

Autoriser RDP uniquement depuis plages IP IT (TCP 3389) — Inbound — Allow — Domain only

```
 # Vérification des règles de blocage en place (audit local)
# Lister les règles MDM actives de blocage
Get-NetFirewallRule | Where-Object {
    $_.PolicyStoreSource -eq "MDM" -and $_.Action -eq "Block"
} | Select-Object DisplayName, Enabled, Direction, Profile | Format-Table -AutoSize

# Vérifier que LLMNR et NetBIOS sont bloqués
$blockedPorts = @(5355, 137, 138)
foreach ($port in $blockedPorts) {
    $rule = Get-NetFirewallRule | Where-Object {
        $_.Action -eq "Block" -and $_.Enabled -eq "True"
    } | Get-NetFirewallPortFilter | Where-Object { $_.LocalPort -eq $port }
    $status = if ($rule) { "BLOQUE" } else { "NON BLOQUE — risque LLMNR/NetBIOS" }
    Write-Host "Port $port : $status"
}
```

Comment valider qu'une règle de pare-feu est bien appliquée sur les postes ?

La validation est une étape souvent négligée. Le portail Intune indique si la politique est appliquée (statut "Succeeded"), mais ne valide pas que les règles font réellement leur travail sur le poste. C'est là qu'intervient **Test-NetConnection**, l'outil natif PowerShell qui teste la connectivité réseau sans nécessiter l'installation d'outils tiers.

```
 # Tester la connectivité TCP sur un port spécifique
# Test avant déploiement d'une règle de blocage
Test-NetConnection -ComputerName "serveur-cible.domaine.local" -Port 445
# TcpTestSucceeded: True = port accessible

# Test après déploiement de la règle de blocage (doit retourner False)
Test-NetConnection -ComputerName "serveur-cible.domaine.local" -Port 445 -InformationLevel Quiet
# Attendu: False

# Afficher l'état du pare-feu par profil réseau
Get-NetFirewallProfile | Select-Object Name, Enabled, DefaultInboundAction, DefaultOutboundAction

# Identifier la source d'une règle (MDM Intune vs GPO vs locale)
Get-NetFirewallRule | Where-Object { $_.DisplayName -like "*NetBIOS*" } |
    Select-Object DisplayName, PolicyStoreSource, Enabled, Action | Format-Table

# Lister les règles entrantes permissives sur le profil Public (potentiel risque)
Get-NetFirewallRule -Direction Inbound -Action Allow -Enabled True |
    Where-Object { $_.Profile -like "*Public*" } |
    Get-NetFirewallPortFilter |
    Select-Object @{N='Règle';E={$_.InstanceID}}, Protocol, LocalPort, RemotePort |
    Format-Table -AutoSize
```

Désactiver la fusion des règles locales pour un contrôle strict

Par défaut, Windows fusionne les règles MDM Intune et les règles locales créées par les utilisateurs ou les logiciels installés. Pour un contrôle strict — typique dans les environnements sensibles, les établissements de santé soumis à HDS, ou les organisations préparant une certification ISO 27001 — désactivez cette fusion dans le profil Windows Firewall d'Intune :

Allow Local Firewall Rules : Disabled pour les profils Public et Private

Allow Local IPsec Rules : Disabled

Attention à un piège classique : cette configuration bloque aussi les règles créées automatiquement par des logiciels légitimes. Les imprimantes réseau, les logiciels de vidéoconférence, certains outils de gestion IT créent leurs règles de pare-feu à l'installation. Un

déploiement par phases (pilote sur 20 machines → 100 machines → parc complet) avec monitoring des signalements permet d'identifier ces cas avant la généralisation.

> **RETOUR D'XPÉRIENCE**
>
> Sur un déploiement Intune que j'ai accompagné fin 2025 dans une PME industrielle, la désactivation de la fusion locale a bloqué une application de supervision Schneider Electric qui créait dynamiquement une règle entrante TCP sur le port 9090. L'application refusait de démarrer sans cette règle. La solution : documenter la règle nécessaire, la créer dans le profil Intune Rules avant de désactiver la fusion, puis déployer. Le test pilote sur 15 machines a sauvé le déploiement — sans lui, 200 postes auraient été impactés simultanément.

Surveiller les événements de pare-feu pour la détection d'intrusion

Les journaux pare-feu Windows sont une source précieuse pour le threat hunting. Ils sont stockés dans `%systemroot%\system32\logfiles\firewall\pfirewall.log` (format texte) et dans le journal d'événements **Microsoft-Windows-Windows Firewall With Advanced Security/Firewall** (format Event Log).

Les Event IDs les plus utiles pour la détection :

Event 2004 : une règle de pare-feu a été créée — surveiller les créations hors fenêtres de maintenance

Event 2006 : une règle de pare-feu a été supprimée — suppression d'une règle de blocage = signal d'alerte

Event 2009 : le pare-feu ne peut pas analyser les règles — problème de configuration MDM

Event 5152/5157 : connexion réseau bloquée — dans les logs d'audit réseau avancés

Pour une centralisation vers un SIEM, l'article sur la détection de menaces avec Microsoft Sentinel décrit comment ingérer ces logs depuis les postes Intune. La stratégie d'audit complète M365 est abordée dans notre guide des journaux avancés Microsoft 365.

```
 # Monitorer les créations et suppressions de règles de pare-feu en temps réel
# Chercher les modifications suspectes dans les 24 dernières heures
$since = (Get-Date).AddDays(-1)

# Règles créées
Get-WinEvent -FilterHashtable @{
    LogName = 'Microsoft-Windows-Windows Firewall With Advanced Security/Firewall'
    Id = 2004
    StartTime = $since
} | Select-Object TimeCreated, Message | Format-List

# Règles supprimées (plus critique — peut indiquer une tentative d'évasion)
Get-WinEvent -FilterHashtable @{
    LogName = 'Microsoft-Windows-Windows Firewall With Advanced Security/Firewall'
    Id = 2006
    StartTime = $since
} | Select-Object TimeCreated, Message | Format-List
```

Intégration avec Microsoft Defender for Endpoint et la posture Zero Trust

Le pare-feu Intune s'intègre nativement avec **Microsoft Defender for Endpoint (MDE)**. Quand MDE est déployé, il supervise automatiquement l'état du pare-feu Windows et remonte des alertes dans le portail Microsoft 365 Defender si le pare-feu est désactivé ou si des règles anormales apparaissent.

Les politiques de réduction de surface d'attaque (ASR) de MDE complètent le pare-feu Intune en bloquant des comportements suspects au niveau du processus : exécution de macros Office, injection de code, accès aux credentials LSASS. L'article sur les pratiques de sécurité Microsoft 365 2025 couvre la configuration conjointe MDE et Intune. Pour une vision complète de la posture Zero Trust, notre article Zero Trust Microsoft 365 détaille la stratégie globale.

Dans le contexte de la conformité NIS 2, la gestion centralisée du pare-feu via Intune est une mesure technique de l'article 21 — protection des systèmes d'information et des réseaux — parfaitement documentable pour les audits de conformité. Notre service RSSI externalisé accompagne les PME dans la mise en place de ce type de contrôles.

Questions fréquentes

Les règles Intune Firewall s'appliquent-elles en priorité sur les règles GPO ?

Sur les appareils Hybrid Joined, les deux coexistent dans des espaces de politique séparés. Les règles MDM Intune et les règles GPO s'additionnent par défaut (fusion). Pour que les règles Intune priment strictement, il faut désactiver la fusion locale et s'assurer qu'aucune GPO Active Directory ne vient redéfinir des paramètres contradictoires. Utiliser `gpresult /h` pour voir les GPO appliquées et `Get-NetFirewallRule | Where-Object { $_.PolicyStoreSource -eq "MDM" }` pour voir les règles Intune.

Comment déployer une exception de pare-feu pour une application métier spécifique ?

Dans Endpoint Security > Firewall > Windows Firewall Rules, créez une règle en spécifiant le chemin de l'exécutable (ex: `%ProgramFiles%\MonApp\monapp.exe`) et les ports autorisés. Pour les applications packagées MSIX ou Store, utilisez le *Package family name* plutôt que le chemin. Testez toujours sur un groupe pilote de 10 à 20 machines avant le déploiement général.

Le pare-feu Intune fonctionne-t-il sur Windows Server ?

Les profils Endpoint Security > Firewall ciblent principalement les postes Windows 10/11. Pour Windows Server, la gestion via Intune est partielle — il vaut mieux combiner GPO Active Directory et Microsoft Defender for Cloud pour les serveurs Azure. Sur les serveurs on-premise, les GPO restent la méthode de référence.

Comment identifier les applications qui créent des règles de pare-feu à l'installation ?

Utilisez **Process Monitor** de Sysinternals filtré sur les modifications de la clé registre `HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy`. Toute application écrivant dans cette clé crée des règles de pare-feu. Cette information vous permet de documenter et recréer ces règles dans Intune avant de désactiver la fusion locale.

Que faire si un utilisateur en déplacement se retrouve bloqué par le profil Public trop restrictif ?

Le profil réseau (Domain/Private/Public) est assigné automatiquement par Windows selon des heuristiques (présence d'un DC joignable pour Domain, paramètre utilisateur pour Private, inconnu = Public). Sur des réseaux d'entreprise mal configurés, un poste peut se retrouver en profil Public alors qu'il devrait être en Domain. Solution : configurer **Network Location Awareness** correctement et vérifier que les politiques réseau identifient correctement les réseaux corporate. En cas de blocage urgent, l'utilisateur peut contacter le support pour une règle temporaire déployée via Intune.

Auditer les règles de pare-feu existantes avant le déploiement Intune

Avant de déployer votre politique Intune dans un environnement où des règles GPO existent déjà, un audit des règles en place s'impose. Sans cet audit, vous risquez deux scénarios : soit les règles GPO trop permissives survivent à côté des nouvelles règles MDM (fusion activée), soit vous bloquez des flux légitimes non documentés en désactivant la fusion.

La démarche recommandée est d'exporter toutes les règles actives depuis un ou plusieurs postes représentatifs, de les analyser pour identifier les règles permissives non justifiées, puis de construire la politique Intune à partir de cette base nettoyée.

```
 # Exporter toutes les règles de pare-feu actives vers un CSV pour analyse
$rules = Get-NetFirewallRule -Enabled True | ForEach-Object {
    $portFilter = $_ | Get-NetFirewallPortFilter
    $appFilter = $_ | Get-NetFirewallApplicationFilter
    $addressFilter = $_ | Get-NetFirewallAddressFilter

    [PSCustomObject]@{
        Nom            = $_.DisplayName
        Direction      = $_.Direction
        Action         = $_.Action
        Profil         = $_.Profile
        ProtoPocole    = $portFilter.Protocol
        PortLocal      = $portFilter.LocalPort
        PortDistant    = $portFilter.RemotePort
        Application    = $appFilter.Program
        AdresseDistant = $addressFilter.RemoteAddress
        Source         = $_.PolicyStoreSource
    }
}

# Exporter en CSV pour revue en Excel
$rules | Export-Csv -Path "C:\Temp\firewall-rules-audit.csv" -Encoding UTF8 -NoTypeInformation
Write-Host "Audit exporté : $(($rules).Count) règles actives"

# Filtrer les règles permissives larges (Any protocol, Any port, Allow)
$risky = $rules | Where-Object {
    $_.Action -eq "Allow" -and
    $_.Direction -eq "Inbound" -and
    ($_.PortLocal -eq "Any" -or $_.PortLocal -eq $null)
}
Write-Host "Règles entrantes larges (Any port) : $(($risky).Count)"
$risky | Select-Object Nom, Profil, Application | Format-Table -AutoSize
```

Cet export CSV est aussi utile pour la documentation de conformité. Pour les organisations préparant une audit de sécurité Microsoft 365 ou une certification ISO 27001, disposer de la liste documentée et datée des règles de pare-feu actives est une exigence documentaire courante. La gestion des journaux de sécurité M365 plus généralement est couverte dans notre article sur l'audit avancé des journaux Microsoft 365.

Gérer les exceptions pour les applications de télétravail

Le télétravail a considérablement complexifié la gestion du pare-feu. Les utilisateurs en remote ont des besoins légitimes d'exceptions que le profil Public strict bloquerait : accès au VPN, aux outils de vidéoconférence (Teams, Zoom), aux solutions de prise en main à distance du support IT.

L'approche recommandée est d'exprimer ces exceptions par application plutôt que par port. En ciblant l'exécutable plutôt que le port, vous limitez le risque d'exploitation : si un autre processus tente d'utiliser le même port, il sera bloqué.

```
 # Exemple de règles par application à créer dans le profil Intune Windows Firewall Rules
# (Équivalent PowerShell pour tests locaux avant déploiement Intune)

# Autoriser le client VPN Cisco AnyConnect
New-NetFirewallRule -DisplayName "ALLOW_VPN_AnyConnect" `
    -Direction Outbound -Action Allow `
    -Program "%ProgramFiles%\Cisco\Cisco AnyConnect Secure Mobility Client\vpnui.exe" `
    -Profile Any -Enabled True

# Autoriser Microsoft Teams (port 443 outbound)
New-NetFirewallRule -DisplayName "ALLOW_Teams_HTTPS" `
    -Direction Outbound -Action Allow `
    -Protocol TCP -RemotePort 443 `
    -Program "%LocalAppData%\Microsoft\Teams\current\Teams.exe" `
    -Profile Public -Enabled True

# Autoriser le module de prise en main à distance du support IT
# (remplacer par l'exécutable de votre outil : TeamViewer, AnyDesk, ConnectWise, etc.)
New-NetFirewallRule -DisplayName "ALLOW_RemoteSupport_IT" `
    -Direction Inbound -Action Allow `
    -Protocol TCP -LocalPort 5938 `
    -Program "%ProgramFiles%\TeamViewer\TeamViewer.exe" `
    -Profile Any -Enabled True
```

Ces règles doivent être intégrées dans les profils **Windows Firewall Rules** Intune avant de désactiver la fusion locale. La clé est de les tester d'abord sur le groupe pilote, puis de collecter les signalements des utilisateurs pendant une semaine avant de généraliser. Pour les stratégies

globales de sécurité des accès M365, notre article sur la sécurisation des accès M365 avec MFA complète la protection périmétrique du pare-feu.

Documenter et maintenir les règles de pare-feu dans le temps

Le pare-feu est souvent bien configuré au départ et laissé à l'abandon ensuite. Six mois après, des règles temporaires deviennent permanentes, des exceptions accordées pour un projet pilote restent actives, des ports ouverts pour des applications désinstallées ne sont jamais fermés. Ce phénomène de "firewall sprawl" est documenté dans les frameworks de durcissement comme le CIS Benchmark.

Pour éviter ce piège, mettez en place trois pratiques simples :

Nommage normalisé des règles : préfixe ALLOW_ ou BLOCK_, suffixe avec la date de création (ALLOW_AppMétier_TCP8443_2026Q3). Facilite le tri et l'identification des règles anciennes.

Revue trimestrielle : script PowerShell planifié qui liste les règles et les compare à la liste approuvée — toute règle non dans la liste approuvée génère une alerte.

Documentation des exceptions : chaque exception de pare-feu documentée dans votre CMDB ou outil ITSM avec date d'expiration — les exceptions sans date deviennent permanentes par défaut, ce qui est rarement l'intention.

Le Centre for Internet Security (CIS) publie des benchmarks détaillés pour Windows qui incluent les paramètres pare-feu recommandés par version d'OS. Ces benchmarks servent de référence objective pour les audits de conformité. Pour notre accompagnement sur la mise en conformité NIS 2 et sur les audits de sécurité infrastructure, la vérification des règles pare-feu fait partie des contrôles techniques standards.