FIREWALL TOOLBOX

Rapport complet

Détails de l'appliance

Numéro de série :	0040103CD830
Nom du pare-feu :	UDS-NSV270
Modèle de l'appliance :	SonicWall NSv 270
Temps de fonctionnement :	0 Days, 0 Hours, 22 Minutes, 15 Seconds
Version du firmware :	7.3.0-7012-R8150

Détails du rapport

Créé le :	15.09.2026 16:37:38
Fichier EXP :	C:\Us...ox\Repository\0040103CD830\exp_api_downloaded.exp
Horodatage EXP :	15.09.2026 16:33:48
Fichier TSR :	C:\Us...ox\Repository\0040103CD830\tsr_api_downloaded.wri
Horodatage TSR :	15.09.2026 16:33:49

Informations complémentaires

- IPv6 est désactivé. Les rapports liés à IPv6 ne sont pas inclus

- Les règles ajoutées automatiquement sont exclues de ce rapport

Table des matières

Explication

Alignement de la configuration avec les bonnes pratiques

Ce rapport évalue la configuration actuelle du pare-feu SonicWall par rapport aux recommandations de bonnes pratiques établies. Son objectif est d'identifier les paramètres déjà conformes aux normes opérationnelles et de sécurité, tout en mettant en évidence les domaines où des améliorations pourraient être recommandées. L'évaluation vise à soutenir un examen structuré de la configuration de l'appareil en matière de sécurité, de maintenabilité, de résilience et de fiabilité globale du service.

Une configuration de pare-feu bien alignée aide à réduire le risque opérationnel, simplifie l'administration et améliore la transparence lors des activités de support et d'audit. Outre les contrôles de sécurité techniques, l'alignement sur les bonnes pratiques inclut également la cohérence de la configuration, une identification claire de l'appareil et l'évitement de paramètres inutiles ou hérités. Chaque section examinée dans ce rapport est donc conçue pour fournir à la fois une indication de statut et une brève explication de la pertinence de l'élément évalué du point de vue opérationnel ou sécuritaire.

Une attention particulière est accordée à l'état logiciel et firmware du pare-feu. Le rapport vérifie si le firmware actuellement installé est à jour et si des indices d'une rétrogradation de firmware non prise en charge ont été détectés. Ceci est important car un firmware obsolète peut exposer l'appareil à des problèmes connus, tandis que des scénarios de rétrogradation non pris en charge peuvent affecter la stabilité, la compatibilité et le support du fournisseur. Un état de firmware conforme constitue donc une exigence clé pour un fonctionnement sûr et fiable.

Le rapport examine également si IPv6 est activé et si son utilisation semble appropriée pour l'environnement. Si IPv6 n'est pas nécessaire, il devrait généralement être désactivé afin de réduire la surface d'attaque inutile et la complexité administrative. De même, le rapport évalue si la haute disponibilité est activée. Lorsque la haute disponibilité n'est pas utilisée, sa mise en œuvre est fortement recommandée, car elle améliore la résilience et réduit les temps d'arrêt en cas de panne matérielle ou de maintenance planifiée.

Un autre domaine important est la redondance de connectivité. La configuration est examinée afin de déterminer si plusieurs connexions WAN sont disponibles. Si une seule liaison montante WAN est utilisée, une connexion WAN supplémentaire est fortement recommandée afin d'améliorer la redondance et de maintenir la connectivité Internet lors des pannes du fournisseur. Les paramètres d'optimisation liés au WAN, tels que le MTU, sont également pris en compte. Si le MTU WAN semble configuré de manière inhabituellement basse, cela devrait être examiné, car des valeurs de MTU inutilement basses peuvent réduire l'efficacité de la transmission et nuire aux performances.

D'un point de vue sécurité, le rapport inclut des vérifications liées à la protection des comptes utilisateurs, au renforcement du VPN et aux capacités de défense contre les menaces. Il évalue si les comptes administratifs sont protégés par une authentification à deux facteurs, fortement recommandée pour réduire le risque d'accès non autorisé via des identifiants faibles, réutilisés ou compromis. La configuration VPN est également examinée afin de détecter la présence d'algorithmes de chiffrement obsolètes, de chiffrements faibles ou de paramètres hérités susceptibles de réduire la sécurité des communications chiffrées. En outre, le rapport vérifie si les fonctions de détection et de prévention sont activées, ces fonctions étant essentielles pour identifier une activité suspecte et bloquer les menaces potentielles à un stade précoce.

La visibilité administrative et la discipline opérationnelle sont en outre traitées via des vérifications telles que la journalisation d'audit interne et le statut de la capture de paquets. Une fonction d'audit interne activée est importante car elle assure la traçabilité des modifications de configuration et des actions administratives, ce qui facilite le dépannage, les enquêtes de sécurité et les exigences de conformité. Le rapport indique également si la capture de paquets est toujours en cours d'exécution. Une capture de paquets activée en continu peut indiquer un dépannage inachevé et peut entraîner une surcharge inutile si elle reste activée sans raison opérationnelle valable.

Enfin, le rapport prend en compte l'état d'utilisation global du pare-feu. L'examen de l'utilisation globale est important pour déterminer si l'appareil fonctionne dans une plage de charge acceptable ou approche de ses limites de capacité. Une utilisation constamment élevée peut indiquer des risques de performance et devrait être évaluée plus en détail. Ensemble, les constats de ce rapport offrent un aperçu pratique de la qualité de la configuration actuelle et aident à identifier les mesures susceptibles d'améliorer la posture de sécurité, la stabilité opérationnelle et la maintenabilité à long terme.

Le nom du pare-feu a été modifié

Renommer un pare-feu SonicWall de son numéro de série vers un nom d'appareil significatif améliore l'administration, le dépannage et les rapports. Un nom descriptif facilite l'identification en un coup d'œil de l'emplacement, du rôle ou de l'attribution client du pare-feu, en particulier dans les environnements comportant plusieurs appareils. Cela réduit la confusion, accélère les activités de support et diminue le risque d'erreurs de configuration ou opérationnelles.

Fonction - Paramètre	Statut	Recommandation
Le nom du pare-feu a été modifié	Statut	-

Firmware et paramètres

Cette section indique si la version de firmware actuelle est utilisée et si une rétrogradation de firmware non prise en charge a été détectée. Cela permet d'évaluer rapidement l'état du logiciel et d'identifier les risques potentiels pour le fonctionnement, la compatibilité et le support.

Fonction - Paramètre	Statut	Recommandation
La version du firmware est à jour	mise à jour disponible	Mettre à jour le firmware

Rétrogradation de firmware non prise en charge

Il s'agit d'une vérification permettant de déterminer si une rétrogradation de firmware non prise en charge s'est produite

Fonction - Paramètre	Statut	Recommandation
Rétrogradation de firmware non prise en chargenon détecté		-

Statut IPv6

Si IPv6 n'est pas nécessaire dans l'environnement, il doit être désactivé afin de réduire la surface d'attaque inutile et la complexité administrative.

Fonction - Paramètre	Statut	Recommandation
Statut IPv6	désactivé	-

Statut de haute disponibilité

Si la haute disponibilité n'est pas activée, son utilisation est fortement recommandée afin d'améliorer la résilience et de réduire les temps d'arrêt en cas de panne matérielle ou de maintenance. Cela aide à garantir la continuité du service et augmente la disponibilité globale de l'infrastructure de sécurité.

Fonction - Paramètre	Statut	Recommandation
Statut de haute disponibilité	présent	-

Lignes WAN redondantes

Si une seule connexion WAN est utilisée, une ligne WAN supplémentaire est fortement recommandée afin d'améliorer la redondance et de maintenir la connectivité Internet en cas de panne du fournisseur. Plusieurs connexions WAN augmentent également la disponibilité globale et peuvent prendre en charge le basculement ou la répartition de charge.

Fonction - Paramètre	Statut	Recommandation
Lignes WAN redondantes	configuré	-

Configuration VPN

Cette section met en évidence les problèmes potentiels dans la configuration VPN, tels que des algorithmes de chiffrement obsolètes, des chiffrements faibles ou des paramètres hérités. Ces constats peuvent réduire la sécurité globale de la connexion VPN et entraîner des problèmes de compatibilité, de conformité ou de support. Il est recommandé de revoir et de mettre à jour la configuration VPN afin de l'aligner sur les normes de sécurité et les bonnes pratiques actuelles.

Fonction - Paramètre	Statut	Recommandation
Algorithmes VPN non sécurisés utilisés	oui	Reconfigurer les tunnels VPN

Audit interne du pare-feu

Cette section indique si la fonction d'audit interne est activée sur le pare-feu SonicWall. Une fonction d'audit activée est importante car elle enregistre les modifications de configuration et les actions administratives, améliorant ainsi la traçabilité et la responsabilité. Cela facilite le dépannage, les enquêtes de sécurité et les exigences de conformité.

Fonction - Paramètre	Statut	Recommandation
Audit interne du pare-feu	activé	-

Compte administrateur intégré utilisé pour l’administration

Si l'audit interne est actif, cette fonction vérifie si l'utilisateur Admin générique a été détecté dans le journal d'audit. Il est recommandé d'utiliser des comptes personnalisés pour l'administration

Fonction - Paramètre	Statut	Recommandation
Compte administrateur intégré utilisé pour l'administration	oui	utiliser des comptes person

Fonctions de détection et de prévention

Cette section indique si les fonctions de détection et de prévention sont activées sur le pare-feu SonicWall.

Fonction - Paramètre	Statut	Recommandation
Fonctions de détection et de prévention	activé	-

Capture de paquets en cours

Cette section indique si la capture de paquets est actuellement toujours en cours d'exécution sur le pare-feu SonicWall.
Une capture de paquets activée en continu doit être examinée, car elle peut indiquer un dépannage inachevé et peut consommer des ressources système ou générer des données de capture inutiles.
Si elle n'est plus nécessaire, elle doit être arrêtée afin d'éviter une surcharge inutile et un impact opérationnel.

Fonction - Paramètre	Statut	Recommandation
Capture de paquets en cours	non	-

Protection des comptes

Cette section indique si les comptes utilisateurs du pare-feu SonicWall sont protégés par une authentification à deux facteurs (2FA).

Fonction - Paramètre	Statut	Recommandation
Compte Admin sécurisé par TOTP	non	Activer le service ou la fonctionnalité
Comptes utilisateurs protégés par TOTP	non	Activer le service ou la fonctionnalité

Utilisation du pare-feu

a surveillance de l'utilisation globale est importante afin d'identifier les situations de charge élevée susceptibles d'affecter les performances, la stabilité ou l'efficacité des services de sécurité.

Fonction - Paramètre	Statut	Recommandation
Utilisation de la dernière minute	0 %	OK
Utilisation de la dernière heure	0 %	OK
Utilisation du dernier jour	0 %	OK
Utilisation du dernier jour	0 %	OK

Services de sécurité sous licence mais non utilisés

Ce rapport indique le nombre de services de sécurité sous licence mais non utilisés

Fonction - Paramètre	Statut	Recommandation
Nombre de services	1	Activer le service ou la fonctionnalité

Service de sécurité non activé

Activer un service de sécurité sur une zone alors que le service lui-même est désactivé globalement n'apporte aucune protection effective. Bien que la configuration de la zone indique que le service est actif, le moteur sous-jacent ne fonctionne pas, de sorte qu'aucune inspection ni filtrage n'est effectué. Cela peut créer un faux sentiment de sécurité et entraîner des politiques de pare-feu mal configurées.

Fonction - Paramètre	Statut	Recommandation
Service de sécurité non activé	oui	Activer le service ou la fonctionnalité

Paramètres WAN MTU

Une MTU WAN correctement configurée est importante pour garantir une transmission efficace des paquets et une communication réseau stable. Si la valeur MTU est définie trop bas, cela peut réduire le débit, augmenter la surcharge et affecter négativement les performances des applications ou des connexions VPN.

Fonction - Paramètre	Statut	Recommandation
Taille de MTU WAN faible détectée	non détecté	-

Délai d'expiration de la connexion TCP

La modification du délai d'expiration TCP global affecte chaque session TCP traitée par le pare-feu. Il est généralement recommandé de laisser la valeur par défaut inchangée et de n'ajuster les délais que pour des règles d'accès individuelles lorsque cela est nécessaire.

Fonction - Paramètre	Statut	Recommandation
Le délai d'expiration TCP par défaut a été modifiénon détecté		-

Règles de pare-feu non utilisées depuis longtemps

Les règles actuellement inutilisées n'apportent aucune valeur opérationnelle. Afin de maintenir un cadre clair et efficace, ces règles inutilisées devraient être réévaluées et, le cas échéant, supprimées

Type de règle	Nombre d'occurrences
Règles de pare-feu jamais utilisées (IP v4)	0
Règles de pare-feu non utilisées depuis longtemps (IP v4)	21

Règles de pare-feu désactivées

Les règles actuellement inutilisées n'apportent aucune valeur opérationnelle. Afin de maintenir un cadre clair et efficace, ces règles inutilisées devraient être réévaluées et, le cas échéant, supprimées

Type de règle	Nombre d'occurrences
Règles de pare-feu désactivées (IP v4)	0

Règles de pare-feu autorisant l'accès du WAN vers les réseaux internes

Les règles de pare-feu autorisant l'accès du WAN vers le réseau interne augmentent l'exposition et devraient être limitées aux seuls services essentiels, avec une validation régulière du besoin métier

Type de règle	Nombre d'occurrences
Règles de pare-feu autorisant l'accès du WAN vers les réseaux internes (IP v4)	0

Règles ANY <> ANY

Les règles autorisant toute source vers toute destination sur tout port créent une exposition excessive et devraient être évitées, sauf en cas de besoin métier clairement justifié et documenté.

Type de règle	Nombre d'occurrences
Règles ANY <> ANY (IP v4)	0

Règles autorisant l'accès d'administration

Les règles autorisant l'accès d'administration devraient être strictement limitées aux sources autorisées et aux services sécurisés, car elles présentent un risque élevé si elles sont exposées trop largement.

Type de règle	Nombre d'occurrences
Règles autorisant l'accès d'administration (IP v4)	4

Politiques NAT inutilisées

Les politiques NAT inutilisées ne remplissent aucune fonction active et devraient être régulièrement revues afin de déterminer si elles sont encore nécessaires ou peuvent être supprimées.

Type de règle	Nombre d'occurrences
Politiques NAT inutilisées (IP v4)	0

Politiques NAT désactivées

Les politiques NAT inutilisées ne remplissent aucune fonction active et devraient être régulièrement revues afin de déterminer si elles sont encore nécessaires ou peuvent être supprimées.

Type de règle	Nombre d'occurrences
Politiques NAT désactivées (IP v4)	0

Informations complémentaires

- Les règles ajoutées automatiquement sont exclues de ce rapport

Rapport de sécurité

Explication

L'audit de sécurité se concentre sur l'identification des risques de sécurité potentiels et des faiblesses des politiques. Il analyse les règles de pare-feu à la recherche de configurations trop permissives, détecte les objets inutilisés ou risqués, et examine les privilèges utilisateurs et les droits d'accès. L'objectif est de mettre en évidence les erreurs de configuration susceptibles d'être exploitées ou qui enfreignent les bonnes pratiques, en fournissant des informations exploitables pour améliorer la posture de sécurité globale.

Rapport des paramètres d'audit

Explication

Audit interne du pare-feu
L'audit interne des pare-feu est un élément essentiel pour maintenir l'intégrité opérationnelle, la responsabilisation et la sécurité au sein d'un environnement réseau. Le pare-feu représente l'un des points de contrôle les plus critiques d'une organisation, et l'audit offre une visibilité sur les modifications de configuration, les événements d'accès et les actions administratives qui influencent directement la posture de sécurité du réseau.

Responsabilisation et traçabilité
Les journaux d'audit documentent qui a effectué les modifications, quand elles ont été effectuées et ce qui a été modifié. Cette traçabilité garantit que les responsabilités sont clairement attribuées et que toute erreur de configuration, tout écart par rapport aux normes ou tout changement non autorisé peut être rapidement identifié et corrigé.

Détection des modifications non autorisées ou risquées
Les pare-feu influencent directement le contrôle d'accès, la protection des données et le flux de trafic. L'audit interne permet aux administrateurs de détecter les modifications de configuration intentionnelles ou accidentelles, aidant à identifier les incidents de sécurité, les violations de politiques ou les utilisations abusives potentielles des privilèges administratifs.

Soutien à la conformité et à la gouvernance
De nombreux cadres réglementaires exigent l'audit des systèmes critiques tels que les pare-feu. Les enregistrements d'audit interne soutiennent la conformité aux normes pertinentes pour des secteurs tels que la finance, la santé et le gouvernement. Ils fournissent la preuve que les politiques sont suivies et que les mécanismes de protection sont correctement appliqués.

Aperçu opérationnel et amélioration continue
Les journaux d'audit aident les équipes de sécurité à comprendre l'historique de configuration et les tendances opérationnelles. L'examen régulier de ces enregistrements permet aux organisations d'affiner leurs politiques d'accès, d'identifier les problèmes récurrents et de renforcer les pratiques de gestion des changements.

Investigation des incidents et analyse forensique
Lorsqu'un événement de sécurité survient, les données d'audit interne constituent souvent l'une des sources de preuves les plus précieuses. Elles permettent aux enquêteurs de reconstituer les actions effectuées sur le pare-feu, d'analyser les causes profondes et de déterminer si une activité malveillante ou une erreur humaine a contribué à l'incident.

Conclusion
L'audit interne est nécessaire pour garantir la transparence, la cohérence et la responsabilisation dans les opérations du pare-feu. Il renforce la sécurité, soutient les exigences réglementaires, permet un dépannage plus rapide et constitue une base essentielle pour une gestion réseau résiliente.

Rapport des paramètres d'audit

Audit Details

Audit interne : on

Enregistrements d'audit trouvés dans le rapport TS :2000

Entrée d'audit la plus récente trouvée dans le rapport TS :15.09.2026 16:33:49

Entrée d'audit la plus ancienne trouvée dans le rapport TS27.07.2026 08:29:20

Utilisateurs identifiés dans le journal d'audit

- UDSAdmin
- admin
- apiuser
- HA Sync

Informations complémentaires

Utilisation d'un compte administrateur générique

Le compte utilisateur *« admin »* a été détecté dans les enregistrements d'audit. Il est recommandé d'éviter d'utiliser des comptes administrateur génériques ou partagés pour la gestion du pare-feu. Chaque administrateur devrait plutôt se connecter à l'aide d'un compte personnalisé.

L'utilisation d'identités utilisateur individuelles garantit que les modifications de configuration peuvent être tracées

Commentaire
Le compte *HA Sync* est un utilisateur système interne utilisé exclusivement pour synchroniser les données de configuration et opérationnelles entre les appliances dans une configuration haute disponibilité (HA). Ce compte n'est pas destiné à une connexion manuelle ou à un usage administratif.

Rapport des règles avec DPI SSL désactivé

Explication

Règles avec Deep Packet Inspection désactivée
La Deep Packet Inspection (DPI) permet au pare-feu d'analyser le trafic au-delà des informations de connexion de base telles que la source, la destination et le port. Elle constitue un élément important pour l'application des services de sécurité et la détection des menaces dans le trafic réseau.
Ce rapport identifie les règles d'accès pour lesquelles la Deep Packet Inspection est désactivée. Le trafic correspondant à ces règles peut contourner l'inspection basée sur la DPI et, par conséquent, ne pas bénéficier de tous les services de sécurité configurés.
La désactivation de la DPI peut être appropriée pour certains types de trafic, par exemple pour des raisons de compatibilité, de performances ou lorsque le trafic concerné ne nécessite pas d'inspection supplémentaire. Toutefois, la DPI ne devrait normalement être désactivée que de manière intentionnelle et pour une raison documentée.
Examinez les règles répertoriées dans ce rapport et vérifiez que la désactivation de la DPI est nécessaire. En l'absence de raison spécifique, envisagez d'activer la DPI afin de garantir que le trafic bénéficie du niveau d'inspection de sécurité prévu.

Règles pour lesquelles l'inspection Client DPI SSL est désactivée

Ena	A	Name	SrcZone	DstZone	SrcNet	DstNet	SrcSvc	DstSvc	DPI Disabled
YES	A	Allow WAN1	LAN	WAN	KlausMeier	any	any	any	True
YES	A	Heating Maintenance	WAN	LAN	any	LAN Subnets	any	SSH	True

- Les règles ajoutées automatiquement sont exclues de ce rapport

Nombre d'enregistrements : 2

Déchiffrement DPI-SSL client

Explication

L’inspection Client DPI-SSL est une fonction de sécurité essentielle qui permet au pare-feu d’inspecter le trafic HTTPS sortant chiffré. Sans déchiffrement, les services de sécurité tels que Gateway Anti-Virus, Intrusion Prevention, Capture ATP, Content Filtering et Application Control disposent d’une visibilité limitée sur les connexions chiffrées, ce qui peut permettre à certaines menaces d’échapper à l’inspection.
Ce rapport vérifie si l’inspection Client DPI-SSL est sous licence et activée sur le pare-feu. Il identifie également les zones dans lesquelles l’inspection Client DPI-SSL est active et met en évidence les règles d’accès pour lesquelles DPI-SSL a été explicitement désactivé. Les exceptions au niveau des règles doivent être examinées attentivement, car elles peuvent créer des angles morts dans lesquels le trafic chiffré n’est pas inspecté et où les services de sécurité ne peuvent pas être appliqués intégralement.
Les organisations doivent s’assurer que l’inspection Client DPI-SSL est activée lorsque cela est approprié et que les exceptions sont limitées aux applications ou services présentant des exigences de compatibilité documentées. Un examen régulier de la configuration DPI-SSL contribue à maintenir la visibilité sur le trafic chiffré et à réduire le risque de menaces non détectées.

Déchiffrement DPI-SSL client

```
DPI SSL Licensed:          yes
```

```
Le déchiffrement SSL pour le trafic sortant est désactivé (!)
```

Déchiffrement DPI-SSL client

Zone	DPI SSL Client
LAN	On
WAN	Off
DMZ	Off
VPN	Off
SSLVPN	Off
MULTICAST	Off
DMZ-unsec	Off
DMZ-sec	Off
Test	On
150971-Test	Off
060466	Off

Règles pour lesquelles l'inspection Client DPI SSL est désactivée

Ena	A	Name	SrcZone	DstZone	SrcNet	DstNet	SrcSvc	DstSvc	DPI-SSL Client Disabled
YES	A	Heating Maintenance	WAN	LAN	any	LAN Subnets	any	SSH	True
YES	A	Complicated Rule	DMZ-unsec	Test	any	any	Citrix UDP	any	True
YES	A	Rule6	DMZ-sec	Test	any	Test13	Citrix TCP	any	True

- Les règles ajoutées automatiquement sont exclues de ce rapport

Nombre d'enregistrements : 3

Fonctions de détection et de prévention

Explication

Les options Randomize IP ID et Enable Stealth Mode offrent une protection supplémentaire contre la reconnaissance réseau et certaines classes d'attaques. La randomisation du champ IP Identification complique le fingerprinting du système d'exploitation ou la déduction des schémas de trafic par les attaquants, tandis que le mode furtif (Stealth Mode) empêche le pare-feu de répondre aux tentatives de connexion non sollicitées, réduisant ainsi sa visibilité sur les réseaux non fiables.

Fonctions de détection et de prévention

Mode furtif (Stealth Mode)

Mode furtif activé	on

Randomize IP ID

Randomize IP ID activé	on

Règles autorisant toute destination et tout port (IPv4)

Explication

Pourquoi les règles de pare-feu autorisant "Any" (tout) sont risquées
Dans le domaine de la sécurité réseau, les règles de pare-feu jouent un rôle essentiel dans le contrôle du trafic entrant et sortant d'un réseau. Une pratique courante, mais fortement déconseillée, est la mise en œuvre de règles « de tout vers tout ». Ces règles permettent un flux de trafic sans restriction depuis n'importe quelle source vers n'importe quelle destination, autorisant essentiellement tous les types de paquets de données à traverser le pare-feu sans aucun filtrage.

Implications en matière de sécurité *La principale préoccupation liée aux règles « de tout vers tout » est le risque de sécurité important qu'elles représentent. Les pare-feu sont conçus pour agir comme des gardiens, examinant le trafic entrant et sortant afin de protéger le réseau contre les accès non autorisés, les cyberattaques et autres activités malveillantes. En définissant des règles qui autorisent tout le trafic sans distinction, la fonction essentielle du pare-feu est contournée, exposant le réseau à des menaces potentielles. Cette porte ouverte peut être exploitée par des attaquants pour accéder à des informations sensibles, injecter des logiciels malveillants ou lancer d'autres exploits préjudiciables.*

Manque de contrôle du trafic *Outre les vulnérabilités de sécurité, les règles « de tout vers tout » entravent la capacité à surveiller et contrôler efficacement le trafic réseau. Une gestion réseau efficace repose sur la compréhension et la gestion du flux de données. Des règles sans restriction rendent difficile le suivi, l'analyse ou la priorisation du trafic, entraînant des problèmes potentiels de performance réseau, notamment une congestion de la bande passante et une efficacité réduite.*

Conformité et bonnes pratiques *Dans de nombreux secteurs, les exigences réglementaires imposent un contrôle et une surveillance stricts du trafic de données. Les règles « de tout vers tout » peuvent enfreindre les normes de conformité, entraînant des répercussions juridiques et réputationnelles. De plus, les bonnes pratiques en cybersécurité prônent un principe du moindre privilège, où seul le trafic nécessaire est autorisé, soulignant davantage le caractère déconseillé de telles règles permissives.*

Recommandation *Plutôt que d'adopter des règles « de tout vers tout », il est recommandé de mettre en œuvre des règles de pare-feu spécifiques et bien définies, basées sur le principe du moindre privilège. Ces règles doivent être conçues pour n'autoriser que le trafic nécessaire et légitime requis pour les opérations commerciales, garantissant à la fois la sécurité du réseau et des performances optimales.*

Règles autorisant toute destination et tout port (IPv4)

Ena	A	Name	SrcZone	DstZone	SrcNet	DstNet	SrcSvc	DstSvc	
YES	A	Allow WAN1	DMZ-sec	WAN	any	any	Enhanced TV	any	
YES	A	Complicated Rule	DMZ-unsec	Test	any	any	Citrix UDP	any	
YES	A	Allow WAN1	DMZ-unsec	WAN	any	any	Citrix UDP	any	
YES	A	Allow Citrix	any		any	any	Citrix UDP	any	Example any<> any
YES	A	Allow FTP	any		any	any	FTP	any	

- Les règles ajoutées automatiquement sont exclues de ce rapport

Nombre d'enregistrements : 5

Règles de pare-feu autorisant les services d'administration depuis des réseaux non fiables (IPv4)

Explication

Règles de pare-feu autorisant les services d'administration depuis des réseaux non fiables
Les services d'administration tels que SSH (Secure Shell), HTTPS (Hypertext Transfer Protocol Secure) et les interfaces d'administration similaires sont destinés à un accès privilégié. Les autoriser directement depuis des réseaux non fiables engendre de multiples problèmes de sécurité.

Pourquoi ces règles sont risquées :
Exposition aux attaques
Autoriser l'accès aux services d'administration via Internet les expose à des attaques telles que des tentatives de connexion par force brute, l'exploitation de vulnérabilités logicielles ou des attaques par déni de service ciblant le service.

Élévation de privilèges
Si un attaquant parvient à se connecter à un service d'administration, il peut obtenir un accès de niveau administrateur. Cela pourrait lui permettre de modifier les configurations du pare-feu, de créer des mécanismes d'accès persistants ou d'interrompre les communications réseau.

Interception et espionnage (sniffing)
Les protocoles d'administration non chiffrés peuvent permettre aux attaquants d'intercepter des informations sensibles. Même les services chiffrés peuvent être à risque si les clés sont exposées, si un chiffrement obsolète est utilisé ou si des failles d'implémentation existent.

Manque de surveillance
Les interfaces d'administration ne sont souvent pas surveillées aussi rigoureusement que les systèmes destinés aux utilisateurs, ce qui augmente le risque qu'un accès non autorisé passe inaperçu.

Complexité et erreur humaine
Plus le nombre de services exposés en externe est élevé, plus le risque d'erreur de configuration ou d'erreur opérationnelle est important, ce qui peut entraîner une exposition accidentelle de systèmes critiques.

Bonnes pratiques recommandées
L'accès d'administration doit être strictement limité aux réseaux internes fiables. Si une administration à distance est nécessaire, elle doit s'effectuer via des canaux d'accès sécurisés tels que des connexions VPN avec un chiffrement fort. L'authentification multifacteur doit être mise en œuvre dans la mesure du possible, les services d'administration doivent être activement surveillés pour détecter les tentatives d'accès non autorisées, et les appareils doivent être maintenus à jour avec les correctifs actuels afin d'atténuer les vulnérabilités connues.

Règles de pare-feu autorisant les services d'administration depuis des réseaux non fiables (IPv4)

Ena	A	Name	SrcZone	DstZone	SrcNet	DstNet	SrcSvc	DstSvc
YES	A	Test 24	WAN	060466	any	any	any	OSPF
YES	A	Test 25	WAN	060466	any	any	any	POP3 (Retrieve E-Mail)
YES	A	Test 23	WAN	060466	any	any	any	MSN
YES	A	Heating Maintenance	WAN	LAN	any	LAN Subnets	any	SSH Temp, Rule to allow M...

- Les règles ajoutées automatiquement sont exclues de ce rapport

Nombre d'enregistrements : 4

Options d'accès à l'administration

Explication

Options d'accès à l'administration et considérations de sécurité

Plusieurs méthodes sont disponibles pour accéder à l'administration du pare-feu, chacune offrant des avantages d'utilisabilité et des implications de sécurité différents. Étant donné que les interfaces d'administration du pare-feu offrent un contrôle administratif sur une infrastructure réseau critique, une exposition inappropriée de ces méthodes d'accès peut engendrer un risque important.

Un accès non autorisé à l'administration du pare-feu peut entraîner la manipulation de la configuration, la divulgation de paramètres de sécurité sensibles, voire la compromission complète de l'environnement réseau. Pour cette raison, il est essentiel de vérifier régulièrement quels mécanismes d'accès d'administration sont activés et de s'assurer que seules des méthodes sûres, justifiées et correctement protégées restent accessibles.

Restreindre l'accès d'administration aux réseaux fiables, imposer une authentification forte et surveiller l'activité administrative sont des pratiques clés pour maintenir un paysage de configuration sécurisé et contrôlé.

Options d'accès à l'administration

Central Management

Central Management (NSM / GMS):	off
NSM ZeroTouch:	enabled

SSL-VPN

SSL VPN Web Management:	on
SSL VPN SSH Management:	off

API

API access:	enabled

Options d'accès à l'administration: Gestion des interfaces

Interface	Zone	HTTP	HTTPS	PING	SSH	SNMP	API
X0	LAN	off	on	on	on	on	on
X1	WAN	off	on	on	on	off	on
X2	DMZ-unsec	off	on	on	off	off	on
X3	DMZ-sec	off	on	on	off	off	on
X4	HA Data & Control	off	off	off	off	off	off
X5	WAN	off	off	on	off	off	off
X6	LAN	off	on	on	off	off	on
X7	DMZ-sec	off	off	off	off	off	off
X6:V100	LAN	off	off	off	off	off	off

Options d'accès à l'administration: IPSec (VPN)

Tunnel-Name	Enabled	HTTP	HTTPS	SSH	SNMP
WAN GroupVPN	False	off	off	off	off
SNWL Policy Mode	False	off	on	on	on
Test	False	off	off	off	off
Bad Tunnel	False	off	off	off	off
To TZ570	True	off	off	off	off
Remote Site1	True	off	off	off	off
New York	True	off	off	off	off

Services de sécurité - Vue d'ensemble activés et désactivés

Explication

Services de sécurité actifs
Ce rapport indique quels services de sécurité sont actuellement activés sur l'appareil. Cependant, l'activation au niveau du système indique seulement que la fonctionnalité du service est disponible - elle ne garantit pas que le trafic est réellement inspecté.

Pour analyser efficacement le trafic, les services de sécurité doivent également être explicitement attribués à des zones ou appliqués à des règles de pare-feu spécifiques. Sans cette étape de configuration, les technologies activées peuvent rester inactives pour les flux réseau pertinents, entraînant une couverture de protection réduite.

Statut du service de sécurité

Deep Packet Inspection for SSL (DPI-SSL)	Off
Gateway AV	On
Anti-Spyware	On
Intrusion Prevention	On
App Control	On
Content Filtering Service	On
GeoIP Filtering	On

Informations complémentaires

Aucun tunnel VPN « route-all » configuré

Aucun tunnel VPN acheminant tout le trafic (route-all) n'est actuellement configuré et actif. Il s'agit d'un scénario courant dans les environnements où tout le trafic est transmis à un dispositif de sécurité en amont, responsable de l'inspection du trafic, de l'application des politiques et du traitement de sécurité supplémentaire.

Dans de telles configurations, le pare-feu fonctionne principalement comme un dispositif de routage ou de segmentation, tandis que l'inspection plus approfondie est gérée par une solution de sécurité centralisée, telle qu'une passerelle web sécurisée, un service de sécurité cloud ou une plateforme d'inspection dédiée.

Services de sécurité - Attribution par zone

Explication

Services de sécurité
Ce rapport indique quels services de sécurité sont activés sur chaque zone. Bien que l'activation d'un service au niveau global rende sa fonctionnalité disponible, la protection réelle n'est appliquée que si le service est activement attribué au niveau de la zone.

Les services de sécurité liés aux zones déterminent quels segments réseau bénéficient d'une inspection contre des menaces telles que les logiciels malveillants, les tentatives d'intrusion ou le contenu indésirable. Les zones sans attribution de service correspondante peuvent rester insuffisamment protégées, même si la fonctionnalité est activée au niveau du système.

Cette vue d'ensemble aide à identifier les lacunes de couverture, à vérifier que les zones critiques (comme le LAN ou les zones d'accès VPN) sont correctement protégées, et à garantir que les politiques d'inspection sont alignées sur les exigences de sécurité de l'organisation.

Informations complémentaires

Les services de sécurité marqués d'un (!) sont activés sur la zone mais désactivés globalement.

Services de sécurité - Attribution par zone

Zone	ClientAV	GatewayAV	IPS	AntiSpyware	DPI SSL Client	DPI SSL Server	SSLControl
LAN	Off	On	On	On	On (!)	Off	Off
WAN	Off	On	On	On	Off	On (!)	Off
DMZ	Off	Off	Off	Off	Off	Off	Off
VPN	Off	Off	Off	Off	Off	Off	Off
SSLVPN	Off	Off	Off	Off	Off	Off	Off
MULTICAST	Off	Off	Off	Off	Off	Off	Off
DMZ-unsec	Off	Off	Off	Off	Off	Off	Off
DMZ-sec	Off	Off	Off	Off	Off	Off	Off
Test	Off	On	On	On	On (!)	Off	Off
150971-Test	Off	Off	Off	Off	Off	Off	Off
060466	Off	On	On	On	Off	Off	Off

Protection des comptes utilisateurs

Explication

Vue d'ensemble de la protection des comptes utilisateurs
Ce rapport répertorie tous les comptes utilisateurs et indique comment ils sont protégés, y compris si l'authentification à deux facteurs (2FA) est activée. Cela aide à vérifier la robustesse des mécanismes d'authentification et à identifier les comptes nécessitant une protection supplémentaire.

Protection des comptes utilisateurs

Nom d'utilisateur	TOTP activé
admin	**NO**
All LDAP Users	NO
apiuser	NO
Isabel	NO
LocalAdmin	YES
mschmitz	NO
Robert	NO
Sylvia	NO
Udo	NO
Uwe	NO
Webadmin	NO

Méthodes d'authentification externe des utilisateurs

Explication

Vue d'ensemble de la configuration de l'authentification externe
Ce rapport répertorie les systèmes d'authentification externes configurés, indique s'ils sont activés, et met en évidence les éventuels problèmes de sécurité liés à leur configuration. L'authentification externe peut renforcer considérablement la gestion des identités utilisateur lorsqu'elle est correctement mise en œuvre, mais une configuration incorrecte peut introduire des risques de sécurité et opérationnels.

LDAP (Lightweight Directory Access Protocol)
Lorsque LDAP est utilisé, les demandes d'authentification sont transmises à un annuaire externe tel que Microsoft Active Directory. L'utilisation de LDAP centralise l'identité des utilisateurs et la gestion des mots de passe, réduisant la dépendance aux comptes locaux. Cependant, l'authentification LDAP doit toujours être sécurisée via TLS (LDAPS). Une communication LDAP non chiffrée expose les noms d'utilisateur, les mots de passe et les informations d'appartenance aux groupes à l'interception, augmentant le risque de vol d'identifiants.

Authentification RADIUS
RADIUS est couramment utilisé pour l'accès VPN et les services d'authentification centralisés. Il prend en charge les méthodes de défi-réponse, la journalisation centralisée et l'application normalisée des politiques d'authentification. Des risques de sécurité surviennent lorsque les secrets partagés sont faibles ou réutilisés sur plusieurs systèmes. De plus, si les serveurs RADIUS deviennent indisponibles, l'accès pourrait être interrompu à moins que des mécanismes de secours appropriés ne soient configurés.

Authentification TACACS+
TACACS+ est généralement utilisé pour l'authentification administrative, en particulier dans les environnements d'entreprise. Il sépare les fonctions d'authentification, d'autorisation et de comptabilisation (AAA), ce qui garantit une activité administrative traçable et un contrôle granulaire des privilèges. Bien que sécurisé par conception, TACACS+ nécessite une configuration adéquate des canaux chiffrés et de clés uniques. Les pannes centrales de TACACS+ peuvent bloquer l'accès administratif à moins qu'une redondance ne soit en place.

Configurer et sécuriser correctement les systèmes d'authentification externes contribue à améliorer la responsabilisation, à réduire la complexité de gestion et à renforcer la sécurité globale des accès. Une révision régulière de la disponibilité, des paramètres de chiffrement, de la correspondance des politiques d'authentification et du comportement de secours garantit des processus d'authentification fiables et sécurisés dans tout l'environnement.

LDAP

Server	Enabled	TLS	UserName
udsserver.uds.local	on	on	UDSReadDir

Radius

Server	Enabled	VPN
10.10.33.11	off	off(!)

Tacacs

Server	Enabled	VPN
1.2.3.4	off	off(!)

Vue d'ensemble des utilisateurs administratifs

Explication

Utilisateur administratif
Ce rapport répertorie tous les utilisateurs disposant de privilèges administratifs. Les comptes dotés de droits administratifs ont un accès élevé aux paramètres de configuration, aux modifications de politiques, aux informations sensibles et aux fonctions de gestion du système.
La revue de ces utilisateurs garantit que seul le personnel autorisé conserve un accès privilégié et soutient la conformité, la responsabilité et les pratiques de contrôle d'accès sécurisées.

Users with Full Admin Rights

UDSAdmin

mschmitz

Webadmin

LocalAdmin

Uwe

apiuser

UDS-SNWL-Admins@uds.local

Users with Limited Admin Rights

- no entries -

Users with Read-Only Admin Rights

Udo

Users with Guest Admin Rights

Robert

Sylvia

Informations complémentaires

Avis important concernant les attributions de groupes LDAP
Si des droits administratifs sont attribués à des groupes LDAP, tous les membres de ces groupes héritent automatiquement des privilèges d'administrateur. Cela signifie que toute modification de l'appartenance LDAP - comme l'ajout de nouveaux utilisateurs ou la synchronisation de structures d'annuaire externes - peut accorder involontairement un accès élevé.

Il est essentiel de revoir régulièrement les attributions de groupes et les appartenances afin de garantir que seul le personnel autorisé reçoit des privilèges administratifs et que le contrôle d'accès reste aligné sur les politiques de sécurité de l'organisation.

Bonnes pratiques pour la sécurité VPN

Explication

Sécurité VPN
Les réseaux privés virtuels (VPN) sont essentiels pour protéger les données sur des réseaux non fiables. Pour rester efficaces, leurs paramètres cryptographiques doivent être révisés et mis à jour régulièrement. Les méthodes obsolètes affaiblissent la sécurité, réduisent la conformité et exposent les organisations à des risques inutiles.

Pourquoi les contrôles réguliers sont importants :

- Sécurité :
Les cybermenaces évoluent rapidement. Les anciennes méthodes de chiffrement ou d'authentification peuvent être compromises avec la puissance de calcul moderne.
- Conformité :
De nombreux secteurs exigent un chiffrement fort pour répondre aux exigences réglementaires.
- Contrôle d'accès :
Une authentification forte empêche l'utilisation non autorisée du VPN.
- Protection des données :
Un chiffrement à jour garantit la confidentialité et l'intégrité des informations sensibles.
- Performance et préparation future :
Les normes plus récentes augmentent non seulement la sécurité, mais aussi l'efficacité et l'évolutivité.

Éléments non sécurisés à éviter :
- Chiffrements symétriques :
DES et 3DES sont obsolètes et vulnérables.
- Groupes Diffie-Hellman (DH) :
Les groupes 1 (768 bits), 2 (1024 bits) et 5 (1536 bits) sont trop faibles.
- Versions IKE :
IKEv1 est obsolète ; IKEv2 est recommandé.
- Fonctions de hachage :
MD5 et SHA-1 sont considérés comme compromis et ne sont plus sûrs.
- Gestion des clés :
Les clés pré-partagées (PSK) faibles ou statiques sont faciles à deviner ou à casser par force brute.

Options sécurisées recommandées

- Chiffrement :
- AES-128 ou AES-256.
- Échange de clés :
- Groupes DH ≥ 2048 bits ou Elliptic Curve Diffie-Hellman (P-256/P-384).
- Protocole :
- IKEv2 pour les configurations VPN modernes.
- Intégrité :
- SHA-256 ou supérieur.
- Authentification :
Préférer les certificats ; si des PSK sont utilisées, employer des clés fortes et aléatoires.

Conclusion
Les VPN ne sont solides que si leurs fondations cryptographiques le sont. En évitant les algorithmes faibles et en adoptant des normes modernes, vous protégez les données sensibles, respectez les exigences de conformité et préparez votre réseau aux défis futurs. Révisez et mettez à jour régulièrement la configuration de votre VPN pour rester en sécurité.

Explication

(!) = non sécurisé © = prudence

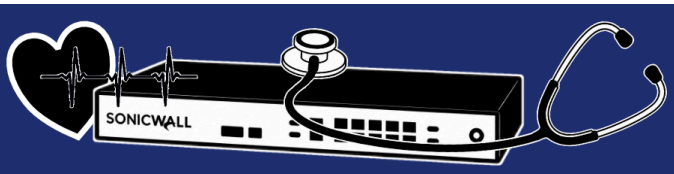
Bonnes pratiques pour la sécurité VPN

Ena	Name	Phase1 Exchange Mode	Phase1 DH-Group	Phase 1 Encr	Phase1 Auth	Phase2 Protcl	Phase2 Encr	Phase2 Auth	Phase 2 PFS	Phase 2 DH-Group
yes	New York	Main (!)	224-Bit R ECP Group	AES-128 (C)	MD5 (!)	ESP	DES (!)	AES-XCBC (C)	off (!)	Group 2 (!)
yes	Remote Site1	IKEv2	Group 2 (!)	AESCGM16-256 (C)	SHA-1 (!)	ESP	AESGMAC-128	n/a	off (!)	Group 2 (!)
yes	To TZ570	IKEv2	Group 1 (!)	AES-256	SHA-1 (!)	ESP	AES-256	n/a	on	n/a

Paramètres cryptographiques de la politique VPN – Algorithmes non sécurisés utilisés

Unsafe		
Category	**Type**	**Comment**
DH Group	192-Bit R ECP Group	Too small ECC group
Encryption	DES	Broken unsafe
IKE	Aggressive	Leads to info leaks insecure
Integrity	MD5	Broken collisions possible
Integrity	SHA-1	Deprecated collision attacks
Misc	None	No encryption integrity

Not recommended		
Category	**Type**	**Comment**
DH Group	224-Bit R ECP Group	Borderline ECC group aging out
Encryption	3DES	Legacy slow 112-bit effective strength
Encryption	AES-XCBC	Niche less common not widely supported
IKE	Main	Standard for IKEv1 secure but older
Protocol	AH	Rarely used integrity only no encryption



Rapport d'état (Health Report)

Explication

Le rapport de maintenance aide à identifier les éléments de configuration qui devraient être examinés régulièrement afin de maintenir le pare-feu propre, efficace et facile à gérer. Au fil du temps, les configurations de pare-feu s'accroissent naturellement à mesure que de nouvelles règles, objets, VPN et services sont ajoutés. Sans maintenance périodique, des entrées obsolètes ou inutilisées peuvent s'accumuler, augmentant la charge administrative et compliquant le dépannage.
Ce rapport met en évidence les éléments de configuration susceptibles de nécessiter une attention particulière, tels que les règles de pare-feu désactivées ou inutilisées, les politiques NAT inactives, les objets d'adresse et de service inutilisés, les services de sécurité expirés et d'autres éléments de configuration qui ne sont plus activement utilisés. Il identifie également les paramètres pouvant bénéficier d'une optimisation ou d'un nettoyage.
L'objectif de ce rapport n'est pas de recommander la suppression automatique de chaque élément répertorié. Il fournit plutôt aux administrateurs une vue d'ensemble structurée des composants de configuration devant être vérifiés avant toute modification. Certains objets ou règles peuvent encore être nécessaires pour des projets futurs, des environnements temporaires, des procédures de reprise après sinistre ou des services rarement utilisés.
Une maintenance régulière offre plusieurs avantages importants :
- Réduit la complexité de la configuration et améliore la lisibilité.
- Facilite considérablement le dépannage et les audits.
- Aide à identifier les éléments de configuration obsolètes ou oubliés.
- Réduit le risque d'erreurs de configuration accidentelles.
- Améliore la gérabilité à long terme du pare-feu.
- Soutient un environnement de sécurité bien documenté et entretenu de manière professionnelle.
Un pare-feu bien entretenu est plus facile à administrer, plus facile à auditer, et constitue une base plus solide pour les futures modifications de configuration et améliorations de sécurité.

Analyse de l'utilisation du pare-feu

Explication

Analyse de l'utilisation du pare-feu
Ces graphiques illustrent le niveau d'utilisation du pare-feu au cours de la période précédant l'exportation des données. Une utilisation élevée peut entraîner une dégradation des performances, notamment un traitement retardé du trafic ou des paquets perdus. Pour obtenir des informations pertinentes, le Technical Support Report utilisé comme source de données devrait idéalement être généré pendant une période de charge système élevée.

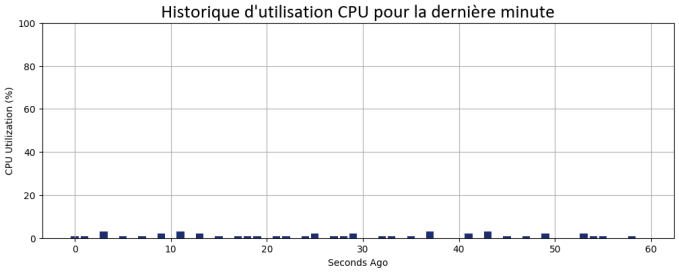
Sources de données recommandées
Des statistiques d'utilisation plus précises sont généralement obtenues à partir de systèmes de surveillance externes basés sur NetFlow ou SNMP. Pour les rapports basés sur NetFlow, SonicWall propose une solution dédiée nommée *Analytics*, qui s'intègre parfaitement aux pare-feu SonicWall.

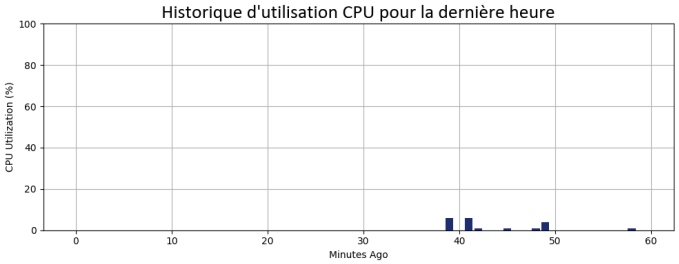
Considérations importantes pour les environnements HA
Si des valeurs d'utilisation sont manquantes pour la période sélectionnée, vérifiez si le pare-feu fonctionne dans un cluster haute disponibilité (HA). Lorsque l'unité de secours devient active pendant la période du rapport, les données d'utilisation peuvent ne pas être capturées sur l'appareil attendu, entraînant des informations graphiques incomplètes ou manquantes.

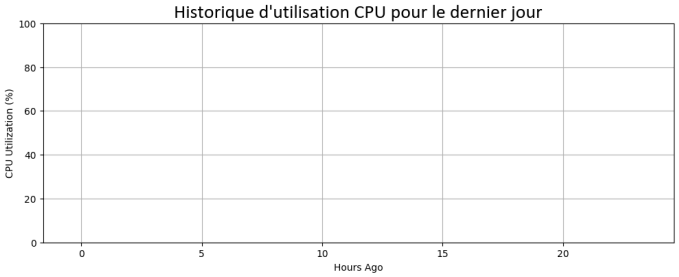
Analyse de l'utilisation du pare-feu

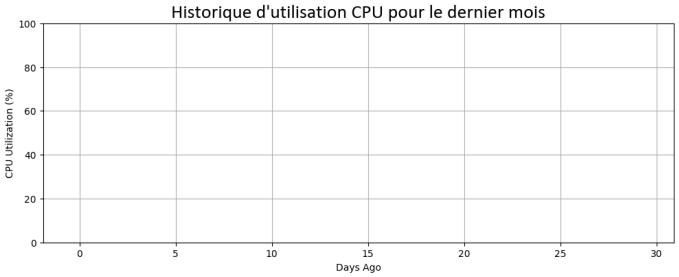
Période	Moyenne	Statut
Minute:	0 %	OK
Heure:	0 %	OK
Jour:	0 %	OK
Mois:	0 %	OK

Graphiques d'utilisation des performances









Firmware Version Check

Explication

Comparaison des versions de firmware
Cette section compare la version de firmware actuellement installée avec la dernière version disponible sur MySonicWall. Cela permet de déterminer si l'appareil est à jour, nécessite une mise à niveau recommandée, ou utilise une version logicielle obsolète qui pourrait manquer d'améliorations, de correctifs de bugs ou d'améliorations de sécurité.

Firmware Version Check:

```
Firmware Installed on Firewall:  7.3.0-7012-R8150
Latest Firmware on MySonicWall:  7.3.3-7015
Firmware Release Date:           26.06.2026
Release Note URL:
https://software.sonicwall.com/Firmware/Documentation/232-006386-00_RevJ_SonicOS_7.3_ReleaseNotes.pdf
```

Informations complémentaires

Le firmware 7.3.3-7015 est disponible sur MySonicWall.com ; envisagez de passer à cette version

Vue d'ensemble de l'historique de configuration et de firmware

Explication

Vue d'ensemble de l'historique de configuration et de firmware
Le tableau suivant donne un aperçu des états de configuration passés et des versions de firmware mises en œuvre sur l'appareil. Il met en évidence la fréquence à laquelle les paramètres ont été migrés et si des rétrogradations de firmware non prises en charge se sont produites.

Rétrogradations non prises en charge
Une rétrogradation de firmware est considérée comme non prise en charge si aucune configuration de la version de firmware rétrogradée n'a été importée par la suite. Dans de tels cas, la compatibilité du système ne peut être garantie, et des problèmes opérationnels peuvent survenir.

Impact des configurations anciennes ou fréquemment migrées
Les configurations qui ont été migrées à plusieurs reprises ou utilisées sur plusieurs appareils peuvent accumuler progressivement des incohérences ou des paramètres obsolètes. Cela peut entraîner un comportement inattendu, des performances dégradées ou des erreurs de traitement de la configuration lors de futures migrations ou mises à niveau.

Firmware	TimeStamp	Action	Comment
7.0.1-5145-2363	24.01.2024 01:33:01	Settings import	
7.1.1-7040-5387	24.01.2024 08:25:53	Firmware applied	
7.1.1-7047-5557	01.03.2024 07:37:45	Firmware applied	
7.1.1-7047-5557	27.11.2024 18:21:03	Settings import	
7.1.1-7058-6162	03.12.2024 20:01:06	Firmware applied	
7.1.1-7058-6162	05.02.2025 21:58:08	Settings import	
7.1.1-7058-6162	21.03.2025 16:23:00	Settings import	
7.1.3-7015-6965	31.03.2025 21:24:27	Firmware applied	
7.3.0-7012-8150	08.09.2025 18:29:24	Firmware applied	
7.3.0-7012-8150	10.03.2026 14:38:34	Settings import	
7.3.0-7012-8150	10.03.2026 16:27:54	Settings import	
7.3.0-7012-8150	11.03.2026 02:01:27	Settings import	
7.3.0-7012-8150	11.03.2026 09:10:26	Settings import	
7.3.0-7012-8150	11.03.2026 11:03:15	Settings import	
7.3.0-7012-8150	21.05.2026 21:28:13	Settings import	

Informations complémentaires

Aucune rétrogradation de firmware non prise en charge détectée

Vue d'ensemble de l'historique de configuration et de firmware

Explication

Vue d'ensemble de la conversion de la configuration
Ce rapport indique si les paramètres de configuration ont été convertis à l'aide de l'outil de conversion de SonicWall. Cela aide à identifier les configurations migrées et donne un aperçu de l'origine des paramètres (plateformes ou déploiements antérieurs).

Details

```
Les paramètres ont été convertis dans le passé : Non
```

Fiabilité - Haute disponibilité

Explication

Importance de la haute disponibilité dans les systèmes de pare-feu

1. Application continue de la sécurité
La haute disponibilité (HA) garantit un fonctionnement ininterrompu des systèmes de pare-feu, en maintenant des contrôles de sécurité continus même en cas de problèmes matériels, de mises à jour ou de maintenance planifiée. Cela évite les lacunes dans la détection des menaces, la validation des accès et l'application des politiques.

2. Réduction des temps d'arrêt
Dans une configuration HA, un pare-feu secondaire prend automatiquement le relais si l'unité principale devient indisponible. Ce basculement transparent minimise les temps d'arrêt, garantissant un accès ininterrompu aux applications et services critiques.

3. Fiabilité système améliorée
Le fait de disposer de plusieurs pare-feu fonctionnant en paire redondante augmente la résilience face aux défaillances matérielles, à la corruption de la configuration ou aux pannes inattendues. La fiabilité de l'infrastructure de sécurité réseau est considérablement améliorée.

4. Soutien à la continuité des activités
Les organisations qui dépendent de la connectivité en temps réel, de l'accès au cloud et des services en ligne ne peuvent pas tolérer des pannes réseau prolongées. La HA protège les opérations commerciales en maintenant l'application de la sécurité active tout au long des événements opérationnels et des scénarios de défaillance.

5. Avantages de performance grâce à la répartition de charge
Certains environnements HA prennent en charge la répartition de charge, améliorant le débit en équilibrant les sessions ou les chemins de trafic sur plusieurs appliances. Cela évite les goulots d'étranglement de traitement et augmente les performances globales du réseau.

6. Capacité de reprise après sinistre
La HA joue un rôle crucial dans la planification de la reprise après sinistre. Lorsqu'un appareil principal tombe en panne, l'unité secondaire maintient actives les politiques, le routage, les tunnels VPN et les services de sécurité, réduisant l'impact opérationnel pendant les activités de récupération.

7. Alignement réglementaire et de conformité
De nombreux secteurs exigent une disponibilité garantie des contrôles de sécurité et des mécanismes de basculement traçables. La mise en œuvre de la HA soutient les initiatives de conformité, la préparation aux audits et les engagements de niveau de service.

8. Meilleure expérience utilisateur et client
Grâce à un accès réseau ininterrompu, les utilisateurs subissent moins d'interruptions de service et bénéficient d'une restauration plus rapide après les pannes. Cela contribue directement à des niveaux de satisfaction plus élevés et à une prestation de service plus stable.

Résumé
La haute disponibilité dans les systèmes de pare-feu constitue un fondement essentiel de la résilience de l'entreprise. Elle garantit une protection continue, minimise les temps d'arrêt opérationnels, soutient la reprise après sinistre, améliore les performances et facilite la conformité. En réduisant les interruptions de service et en maintenant une connectivité sécurisée, la HA renforce considérablement l'efficacité opérationnelle et sécuritaire.

Fiabilité - Haute disponibilité

High Availability Settings

High Availability:	Enabled
HA Primary Serial-Number:	0040103CD830
HA Secondary Serial-Number:	0040103F5B1C
HA Stateful Sync:	Enabled
HA Preempt Mode:	Disabled
HA Control Interface:	X4
HA Data Interface:	X4
HA Role:	Primary
HA Firmware mismatch with peer:	No
HA Active Time:	0 Days 00:21:47

High Availability Status

HA Firewall Status:	Active
HA Peer State:	Peer not found / not active
HA Peer in sync:	No

Informations sur le cycle de vie du produit

Explication

Informations sur le cycle de vie du produit
Cette section donne un aperçu du statut actuel du cycle de vie du produit. Elle aide à déterminer si un appareil est entièrement pris en charge, approche de la fin de son support, ou a déjà dépassé sa période de maintenance officielle.

Pour des descriptions détaillées du cycle de vie, les jalons importants et les calendriers de support actuels, veuillez consulter la documentation officielle sur le cycle de vie des produits SonicWall, disponible via les ressources de support SonicWall.

Description	Value
Model:	SonicWall NSA NSV 270
Last Order Date:	15.04.2022
ARM Begin:	16.04.2022
LRM Begin:	16.04.2024
1 Year LOD:	15.04.2025
End of Support:	16.04.2026

Informations complémentaires

Veuillez revérifier ces informations sur le site Web officiel de SonicWall !

Services de sécurité - Vue d'ensemble du statut de licence

Explication

Licences des services de sécurité
Ce rapport indique quels services disposent actuellement d'une licence active. Les services sous licence sont pleinement fonctionnels et capables de fournir la protection ou l'ensemble de fonctionnalités prévus. Les services sans licence valide peuvent avoir une fonctionnalité limitée ou être complètement inactifs.

Cette vue aide à vérifier si les fonctionnalités de sécurité et basées sur abonnement requises restent opérationnelles, et facilite la planification des renouvellements afin d'éviter les interruptions de service.

Services de sécurité - Vue d'ensemble du statut de licence

Nom du service	Statut de la licence	Nombre	Expiration
Node Upgrade	None		Unlimited
Active/Active Clustering Service	None		Unlimited
NSM Essential (Retired)	Not Licensed		Unlimited
NSM Advanced (Retired)	Disabled		05.02.2026
Capture Client Basic	Not Licensed		Unlimited
Content Filtering Client	None		Unlimited
Capture Client Advanced	Not Licensed		Unlimited
Capture Client Premier	Not Licensed		Unlimited
Deep Packet Inspection for SSL (DPI-SSL)	Licensed		Unlimited
Deep Packet Inspection for SSH (DPI-SSH)	None		Unlimited
Virtual Assist	None		Unlimited
SSL VPN	Licensed	2 Max: 100	Unlimited
Global VPN Client	Licensed	50 Max: 1000	Unlimited
Global VPN Client Enterprise	None		Unlimited
WAN Acceleration Client	None		Unlimited
WAN Acceleration Software	None		Unlimited
Botnet Block	None		Unlimited
Stateful High Availability	Licensed		Unlimited
Comprehensive Anti-Spam Service	None		Unlimited
External IDS Support	None		Unlimited
CSC Analytics (includes Reporting)	None		Unlimited
CSC Management	None		Unlimited
CSC Management Lite	None		Unlimited
CSC Management and Reporting	None		Unlimited
CSC Management and 7-day Reporting	None		Unlimited
Syslog Analytics	Expired		03.02.2024
Comprehensive/Advanced Gateway Security Suite	None		Unlimited
Gateway AV	None		Unlimited
Anti-Spyware	None		Unlimited
Intrusion Prevention	None		Unlimited
App Control	None		Unlimited
App Visualization	None		Unlimited
Content Filtering: Premium Edition	None		Unlimited
Analyzer	None		Unlimited
Capture Advanced Threat Protection	Licensed		14.02.2027
Standard Support	Not Licensed		Unlimited
24x7 Support	Licensed		14.02.2027
SonicOS Expanded	None		Unlimited
Software and Firmware Updates	None		Unlimited
Hardware Warranty	None		Unlimited
Remote Implementation Service	None		Unlimited
Gateway Anti-malware/Intrusion Prevention/App Control	Licensed		14.02.2027
Content Filtering Service	Licensed		14.02.2027
Secure Connect Lite	None		Unlimited
Secure Connect	None		Unlimited
Advanced Reporting & Analytics (7 days)	Licensed		14.02.2027
DNS Filtering	Licensed		14.02.2027

Services de sécurité - Vue d'ensemble du statut de licence

Nom du service	Statut de la licenceNombre	Expiration
Advanced Protection Security Suite	Licensed	14.02.2027
Managed Protection Security Suite	Not Licensed	Unlimited
Web and Chat Only Support	None	Unlimited
Basic Reporting (7 days)	Not Licensed	Unlimited
Essential Protection Service Suite	Disabled	05.02.2026
Advanced Reporting & Analytics	None	Unlimited
Threat Protection Service Suite	None	Unlimited
Model Upgrade	Not Licensed	Unlimited
GeoIP Filtering	None	Unlimited

Fiabilité - Basculement WAN

Explication

Importance du basculement WAN dans les systèmes de pare-feu

1. Connectivité Internet ininterrompue
Le basculement WAN garantit un accès continu à Internet en basculant automatiquement vers une connexion de secours si la liaison WAN principale tombe en panne. Ceci est essentiel pour maintenir les opérations commerciales dépendant de la connectivité Internet.

2. Fiabilité et disponibilité accrues
En fournissant une connexion secondaire, le basculement WAN améliore la fiabilité et la disponibilité des services réseau. Cela réduit les temps d'arrêt et augmente la productivité globale.

3. Continuité des activités
Les pannes réseau peuvent entraîner des pertes financières, une baisse de la satisfaction client et des retards opérationnels. Le basculement WAN soutient la continuité des activités en minimisant les interruptions et en maintenant l'accès aux applications et services critiques.

4. Répartition de charge et performances améliorées
Certaines plateformes de pare-feu prennent en charge à la fois le basculement et la répartition de charge. Cela permet de répartir le trafic sur plusieurs liaisons WAN, optimisant la bande passante et améliorant les performances pour les utilisateurs finaux.

5. Support de la reprise après sinistre
Lors de pannes inattendues ou de défaillances d'infrastructure, le basculement garantit que les processus de récupération restent accessibles et ininterrompus, préservant la disponibilité du service et l'intégrité des données.

6. Maintien de la posture de sécurité
Les pare-feu dotés d'une capacité de basculement garantissent que tout le trafic - en fonctionnement normal comme lors des événements de basculement - continue de passer par les inspections de sécurité. Cela empêche le contournement des mesures de protection pendant les pannes.

7. Efficacité des coûts
Bien que la mise en œuvre de lignes WAN secondaires entraîne des coûts, la prévention des interruptions de service permet d'éviter des pertes financières, une baisse de productivité et une insatisfaction client, générant des économies à long terme.

Résumé
Le basculement WAN est une capacité essentielle des systèmes de pare-feu. Il maintient un accès Internet continu, soutient la reprise après sinistre, améliore la fiabilité, renforce la cohérence de la sécurité et protège la continuité des activités. En réduisant les temps d'arrêt et en améliorant les performances, le basculement WAN aide les organisations à maintenir la qualité du service et l'efficacité opérationnelle.

Fiabilité - Basculement WAN

WAN Interface Summary

Number of WAN Interfaces configured & enabled: 2

Interface	Type	Comment	PacketsIn	PacketsOut
X1	WAN	Default WAN	9268	9071
X5	WAN		1215	328

WAN Load Balancing is: enabled

Interface	Probing	Type	Prim Dest	Protocol	Alt Dest	Protocol
X1	Logical	At least one target should reply	204.212.170.23	TCP	8.8.8.8	ICMP
X5	Physical	None	None	None	None	None

Rapport de configuration

Explication

L'audit de configuration examine la mise en place technique et l'état de préparation opérationnelle de l'environnement du pare-feu. Il évalue des fonctionnalités système telles que la haute disponibilité (HA), le basculement WAN et le statut des services de sécurité. Il vérifie également si les composants clés sont correctement configurés et conformes aux normes de déploiement recommandées.

Délai d’expiration de la connexion TCP

Explication

Le délai d’expiration des connexions TCP détermine la durée pendant laquelle le pare-feu conserve une session TCP inactive dans sa table de connexions avant de la supprimer. La valeur globale par défaut de 15 minutes constitue un réglage approprié pour la plupart des environnements et offre un bon équilibre entre la prise en charge du trafic réseau légitime et la préservation des ressources du pare-feu.
La modification du délai d’expiration TCP global affecte toutes les connexions TCP transitant par le pare-feu. Une augmentation inutile de cette valeur peut entraîner le maintien en mémoire de sessions obsolètes pendant de longues périodes, consommant des entrées dans la table de connexions et réduisant potentiellement la capacité globale de l’équipement. Dans les environnements de grande taille ou à fort trafic, cela peut avoir un impact notable sur les performances du pare-feu et l’utilisation de ses ressources.
Cependant, certaines applications nécessitent des périodes d’inactivité plus longues afin de maintenir des connexions persistantes. Il peut s’agir, par exemple, de certaines applications de bases de données, de logiciels client/serveur anciens ou de systèmes de contrôle industriel spécialisés. Dans ces cas, il est recommandé de conserver le délai d’expiration global à sa valeur par défaut et de configurer un délai d’expiration TCP personnalisé uniquement pour les règles d’accès spécifiques qui le nécessitent.
L’application de délais d’expiration prolongés au niveau des règles présente plusieurs avantages :
Minimise l’impact sur le pare-feu dans son ensemble.
Limite l’augmentation de la consommation des ressources aux applications concernées.
Réduit le nombre de sessions obsolètes dans la table de connexions.
Rend les exigences particulières des applications visibles et plus faciles à documenter.
Simplifie les audits futurs et le dépannage.
Ce rapport présente la configuration actuelle du délai d’expiration TCP global et répertorie toutes les règles d’accès utilisant une valeur de délai d’expiration TCP personnalisée. Les règles comportant des paramètres différents des valeurs par défaut doivent être examinées régulièrement afin de vérifier que l’exception reste nécessaire et qu’elle est correctement documentée.
De manière générale, le délai d’expiration TCP global doit rester à sa valeur par défaut dans la mesure du possible, tandis que les exigences spécifiques des applications doivent être traitées au moyen de délais d’expiration personnalisés au niveau des règles.

General TCP Setting

```
Délai d'expiration global de la connexion TCP : 69
```

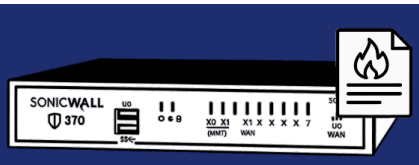
Informations complémentaires

Le délai d’expiration de connexion TCP par défaut a été modifié. Il est recommandé de conserver le paramètre global à 15 minutes. Si un service spécifique nécessite une valeur différente, modifiez le délai d’expiration TCP dans une règle spécifique.

Règles pour lesquelles le délai d’expiration TCP par défaut a été modifié

Ena	A	Name	SrcZone	DstZone	SrcNet	DstNet	SrcSvc	DstSvc	TCP Timeout
YES	A	Rule6	DMZ-sec	Test	any	Test13	Citrix TCP	any	66
YES	A	Complicated Rule	DMZ-unsec	Test	any	any	Citrix UDP	any	10
YES	A	Heating Maintenance	WAN	LAN	any	LAN Subnets	any	SSH	30

Nombre d'enregistrements : 3



Rapport de documentation

Explication

Le rapport de documentation fournit une vue d'ensemble structurée de l'environnement du pare-feu et de ses éléments de configuration clés. Il collecte et présente des informations système pertinentes, notamment les paramètres réseau, les attributions d'interfaces, les configurations de zones et les politiques appliquées.
Ce rapport est conçu pour servir de référence complète aux administrateurs, soutenant à la fois les tâches opérationnelles et le transfert de connaissances. Il garantit que les détails de configuration importants sont clairement documentés et facilement accessibles, réduisant la dépendance à l'inspection manuelle du système.
De plus, la documentation contribue à maintenir la transparence et la cohérence dans l'ensemble de l'environnement, facilitant le dépannage, les audits et les futurs changements.

Tous les enregistrements d'audit

Explication

Audit interne du pare-feu
L'audit interne des pare-feu est un élément essentiel pour maintenir l'intégrité opérationnelle, la responsabilisation et la sécurité au sein d'un environnement réseau. Le pare-feu représente l'un des points de contrôle les plus critiques d'une organisation, et l'audit offre une visibilité sur les modifications de configuration, les événements d'accès et les actions administratives qui influencent directement la posture de sécurité du réseau.

Responsabilisation et traçabilité
Les journaux d'audit documentent qui a effectué les modifications, quand elles ont été effectuées et ce qui a été modifié. Cette traçabilité garantit que les responsabilités sont clairement attribuées et que toute erreur de configuration, tout écart par rapport aux normes ou tout changement non autorisé peut être rapidement identifié et corrigé.

Détection des modifications non autorisées ou risquées
Les pare-feu influencent directement le contrôle d'accès, la protection des données et le flux de trafic. L'audit interne permet aux administrateurs de détecter les modifications de configuration intentionnelles ou accidentelles, aidant à identifier les incidents de sécurité, les violations de politiques ou les utilisations abusives potentielles des privilèges administratifs.

Soutien à la conformité et à la gouvernance
De nombreux cadres réglementaires exigent l'audit des systèmes critiques tels que les pare-feu. Les enregistrements d'audit interne soutiennent la conformité aux normes pertinentes pour des secteurs tels que la finance, la santé et le gouvernement. Ils fournissent la preuve que les politiques sont suivies et que les mécanismes de protection sont correctement appliqués.

Aperçu opérationnel et amélioration continue
Les journaux d'audit aident les équipes de sécurité à comprendre l'historique de configuration et les tendances opérationnelles. L'examen régulier de ces enregistrements permet aux organisations d'affiner leurs politiques d'accès, d'identifier les problèmes récurrents et de renforcer les pratiques de gestion des changements.

Investigation des incidents et analyse forensique
Lorsqu'un événement de sécurité survient, les données d'audit interne constituent souvent l'une des sources de preuves les plus précieuses. Elles permettent aux enquêteurs de reconstituer les actions effectuées sur le pare-feu, d'analyser les causes profondes et de déterminer si une activité malveillante ou une erreur humaine a contribué à l'incident.

Conclusion
L'audit interne est nécessaire pour garantir la transparence, la cohérence et la responsabilisation dans les opérations du pare-feu. Il renforce la sécurité, soutient les exigences réglementaires, permet un dépannage plus rapide et constitue une base essentielle pour une gestion réseau résiliente.

Informations complémentaires

Vue d'ensemble des événements d'audit
Cette section répertorie tous les événements d'audit extraits du Technical Support Report (TSR). Elle offre une visibilité sur les modifications de configuration apportées au pare-feu et identifie les utilisateurs responsables de ces actions.

Remarque importante
Les journaux d'audit ne sont pas synchronisés entre les appliances lorsque la haute disponibilité (HA) est activée. Par conséquent, les modifications effectuées sur l'unité secondaire (active) pendant les périodes de basculement peuvent ne pas apparaître dans la piste d'audit de l'appliance principale. De futures versions de FirewallToolbox pourraient résoudre ce problème !

Ce rapport aide à valider l'activité administrative, favorise la responsabilisation et aide à identifier les modifications de configuration indésirables ou non autorisées.

Informations complémentaires

Ce rapport affiche uniquement les 10 entrées les plus récentes. Exécutez le rapport individuel pour afficher tous les résultats.

Firewall Internal Admin Audit Records

ID: 3749 Timestamp: 15.09.2026 16:33:49
Description: Export Tech Support Report
Old:
New:
Status:
User: UDSAdmin
Session: API
Source: 10.10.10.10 (19526)

ID: 3749 Timestamp: 15.09.2026 16:33:49
Description: Export Tech Support Report
Old:
New:
Status:
User: UDSAdmin
Session: API
Source: 10.10.10.10 (19526)

ID: 3748 Timestamp: 15.09.2026 16:33:49
Description: Export Configuration
Old:
New:
Status:
User: UDSAdmin
Session: API
Source: 10.10.10.10 (19525)

ID: 3748 Timestamp: 15.09.2026 16:33:49
Description: Export Configuration
Old:
New:
Status:
User: UDSAdmin
Session: API
Source: 10.10.10.10 (19525)

ID: 3747 Timestamp: 15.09.2026 16:31:36
Description: Export Tech Support Report
Old:
New:
Status:
User: UDSAdmin
Session: API
Source: 10.10.10.10 (46610)

ID: 3747 Timestamp: 15.09.2026 16:31:36
Description: Export Tech Support Report
Old:
New:
Status:
User: UDSAdmin
Session: API
Source: 10.10.10.10 (46610)

ID: 3746 Timestamp: 15.09.2026 16:31:36
Description: Export Configuration
Old:
New:
Status:
User: UDSAdmin
Session: API
Source: 10.10.10.10 (46608)

ID: 3746 Timestamp: 15.09.2026 16:31:36
Description: Export Configuration
Old:
New:
Status:
User: UDSAdmin
Session: API
Source: 10.10.10.10 (46608)

Firewall Internal Admin Audit Records

```
ID:          3745      Timestamp:   15.09.2026 16:18:33
Description: End Configuration Mode
Old:
New:
Status:
User:        UDSAdmin
Session:     GMS
Source:      127.0.0.1 (50325)
```


```
ID:          3745      Timestamp:   15.09.2026 16:18:33
Description: End Configuration Mode
Old:
New:
Status:
User:        UDSAdmin
Session:     GMS
Source:      127.0.0.1 (50325)
```

Toutes les règles (IPv4)

Explication

Ce rapport fournit un inventaire complet de toutes les règles d'accès IPv4 configurées sur le pare-feu, à l'exclusion des règles d'accès par défaut intégrées. Pour chaque règle, le rapport répertorie l'état d'activation, l'action (Autoriser/Refuser), le nom de la règle, les zones source et destination, les objets réseau source et destination, les objets de service, les commentaires de l'administrateur et l'UUID unique de la règle.
Maintenir un inventaire à jour des règles de pare-feu est un élément essentiel de l'administration du pare-feu et de l'audit de sécurité. Cela permet aux administrateurs de revoir la politique de sécurité mise en œuvre, de vérifier que les règles respectent le principe du moindre privilège, d'identifier les règles obsolètes ou redondantes et de s'assurer que la documentation des règles est complète et pertinente. La révision régulière de la base de règles aide à réduire la complexité de la configuration, améliore le dépannage et minimise le risque d'accès involontaire causé par des règles de pare-feu obsolètes ou trop permissives.

Toutes les règles (IPv4)

Ena	A	Name	SrcZone	DstZone	SrcNet	DstNet	SrcSvc	DstSvc	
YES	A	My Rule	DMZ-sec	DMZ-unsec	any	any	any	FTP Data	
YES	A	Test 17	DMZ-sec	DMZ-unsec	any	any	any	HTTPS	
YES	A	Test 20	DMZ-sec	DMZ-unsec	any	any	any	Kazaa / FastTrack	
YES	A	Test 21	DMZ-sec	DMZ-unsec	any	any	any	Lotus Notes	
YES	A	Test 19	DMZ-sec	DMZ-unsec	any	any	any	IKE	
YES	A	Test 18	DMZ-sec	DMZ-unsec	any	any	any	ICMP	
YES	A	Rule6	DMZ-sec	Test	any	Test13	Citrix TCP	any	
YES	A	Rule10	DMZ-sec	Test	WAN-GoogleDNS-8.8.8.8	any	Direct Connect	any	
YES	A	Allow WAN1	DMZ-sec	WAN	any	any	Enhanced TV	any	
YES	A	Test 22	DMZ-unsec	DMZ-sec	any	any	any	MSN	
YES	A	Allow syslog	DMZ-unsec	DMZ-unsec	any	any	SSH Management	any	
YES	A	Complicated Rule	DMZ-unsec	Test	any	any	Citrix UDP	any	
YES	A	Allow WAN1	DMZ-unsec	WAN	any	any	Citrix UDP	any	
YES	A	Allow WAN1	LAN	WAN	KlausMeier	any	any	any	
YES	A	Allow management via ...	SSLVPN	LAN	SSLVPN-NetExtender Range	any	any	HTTPS Management	
YES	A	Test 24	WAN	060466	any	any	any	OSPF	
YES	A	Test 25	WAN	060466	any	any	any	POP3 (Retrieve E-Mail)	
YES	A	Test 23	WAN	060466	any	any	any	MSN	
YES	A	Heating Maintenance	WAN	LAN	any	LAN Subnets	any	SSH	Temp, Rule to allow M...
YES	A	Allow Citrix	any		any	any	Citrix UDP	any	Example any<> any
YES	A	Allow FTP	any		any	any	FTP	any	

- Les règles ajoutées automatiquement sont exclues de ce rapport

Nombre d'enregistrements : 21

Règles d'administration (IPv4)

Explication

Règles de pare-feu autorisant l'accès d'administration sur les pare-feu SonicWall (SSH / HTTPS)

Les pare-feu SonicWall fournissent des services d'administration tels que SSH et HTTPS pour permettre aux administrateurs de configurer, surveiller et maintenir l'appareil. Ces services accordent un accès privilégié au pare-feu et à ses contrôles de sécurité. Les règles de pare-feu autorisant l'accès d'administration doivent donc être traitées avec une extrême prudence, car une exposition inappropriée peut engendrer de graves risques de sécurité et opérationnels.

Risques de sécurité
Autoriser l'accès d'administration via des règles de pare-feu augmente la surface d'attaque de l'appliance SonicWall. Les interfaces d'administration sont une cible fréquente pour les attaquants, car un accès réussi offre un contrôle administratif direct. Les services SSH ou HTTPS exposés peuvent faire l'objet de tentatives de connexion par force brute, d'attaques de credential stuffing ou de l'exploitation de vulnérabilités dans le plan de gestion SonicWall ou le firmware sous-jacent.

Si un attaquant obtient un accès administratif, il peut modifier les règles du pare-feu, désactiver des services de sécurité, altérer des configurations VPN ou créer des portes dérobées persistantes. De telles actions peuvent entraîner l'interception du trafic, la perte de l'intégrité du réseau ou la compromission complète de l'environnement protégé.

Exposition aux attaques basées sur le réseau
Lorsque les services d'administration SonicWall sont accessibles depuis des réseaux non fiables (comme le WAN ou des zones définies de manière large), ils deviennent visibles pour les analyses automatisées, les activités de reconnaissance et les attaques par déni de service. Même lorsque des protocoles chiffrés tels que HTTPS ou SSH sont utilisés, des risques subsistent si le firmware est obsolète, si des paramètres cryptographiques faibles sont activés, ou si l'accès n'est pas suffisamment restreint.

De plus, des règles d'accès d'administration mal configurées peuvent exposer involontairement des ports administratifs sur plusieurs interfaces ou zones, augmentant la probabilité d'un accès accidentel ou non autorisé.

Impact opérationnel et de conformité
Des règles d'accès d'administration trop permissives compliquent la surveillance et la détection des incidents sur les pare-feu SonicWall. Les tentatives d'accès non autorisées peuvent être difficiles à distinguer d'une activité administrative légitime, en particulier si la journalisation et les alertes ne sont pas configurées de manière stricte. D'un point de vue conformité, un accès d'administration sans restriction ou non documenté enfreint souvent les politiques de sécurité internes et les exigences réglementaires imposant un contrôle strict sur l'accès privilégié et les interfaces administratives.

Bonnes pratiques recommandées pour les pare-feu SonicWall
L'accès d'administration sur les appareils SonicWall doit être limité aux réseaux internes fiables ou à des zones de gestion dédiées. L'accès d'administration direct depuis les interfaces WAN doit être évité autant que possible. Si une administration à distance est nécessaire, elle doit être effectuée via des connexions VPN sécurisées avec une authentification et un chiffrement forts.

D'autres contrôles recommandés incluent la limitation de l'accès par adresse IP source, l'activation de l'authentification multifacteur pour les utilisateurs administratifs, le maintien à jour du firmware SonicWall, et la révision régulière des règles d'accès d'administration et des journaux d'audit. Ces mesures aident à garantir que l'accès administratif reste contrôlé, auditable et conforme aux bonnes pratiques de sécurité SonicWall.

Règles d'administration (IPv4)

Explication

Objets et groupes de services d'administration
Les éléments listés ci-dessous représentent les objets et groupes de services classés comme services d'administration. Ils incluent généralement les protocoles et ports utilisés pour l'accès administratif, la configuration des appareils et les fonctions de surveillance.

L'identification de ces services aide à déterminer où l'accès d'administration est autorisé et garantit que les interfaces administratives ne sont appliquées qu'à des zones fiables et contrôlées du réseau.

Service Objects
Citrix TCP
Citrix TCP (Session Reliability)
Citrix UDP
GMS HTTPS
HTTP
HTTP Management
HTTPS
HTTPS Management
IKE (Key Exchange)
IKE (Traversal)
Kerberos TCP
Ping
SSH
SSH Management
Syslog

Service-Groups
Citrix
Idle HF
Management Services
IKE
Kerberos
Interface Management Services

Règles d'administration (IPv4)

Ena	A	Name	SrcZone	DstZone	SrcNet	DstNet	SrcSvc	DstSvc	
YES	A	Test 17	DMZ-sec	DMZ-unsec	any	any	any	HTTPS	
YES	A	Test 19	DMZ-sec	DMZ-unsec	any	any	any	IKE	
YES	A	Allow management via ...	SSLVPN	LAN	SSLVPN-NetExtender Range	any	any	HTTPS Management	
YES	A	Heating Maintenance	WAN	LAN	any	LAN Subnets	any	SSH	Temp, Rule to allow M...

Nombre d'enregistrements : 4

Interfaces (IPv4)

Explication

Vue d'ensemble de la configuration des interfaces
Ce rapport affiche toutes les interfaces configurées ainsi que leurs paramètres associés. Il offre une visibilité sur les rôles des interfaces, les informations d'adressage et les paramètres opérationnels, aidant à évaluer la connectivité, la segmentation et la structure réseau globale.

Interfaces (IPv4)

Name	Zone	Comment	Assignment	IP	Subnet Mask	Gateway
X0	LAN	Default LAN	Static LAN	10.100.10.254	255.255.255.0	0.0.0.0
X1	WAN	Default WAN	Static	10.10.15.1	255.255.255.0	10.10.15.254
X2	DMZ-unsec		Static LAN	10.100.30.254	255.255.255.0	0.0.0.0
X3	DMZ-sec		Static LAN	10.100.40.254	255.255.255.0	0.0.0.0
X4	HA Data & Control		n/a	n/a	n/a	n/a
X5	WAN		Static	10.10.16.1	255.255.255.0	172.16.1.254
X6	LAN		Static LAN	192.168.1.254	255.255.255.0	0.0.0.0
X6:V100	LAN		Static LAN	192.168.2.254	255.255.255.0	0.0.0.0
X7	DMZ-sec		Static LAN	192.169.1.1	255.255.255.0	0.0.0.0

Nombre d'enregistrements : 9

Vue d'ensemble de l'appartenance des utilisateurs et des groupes

Explication

Utilisateurs et appartenances aux groupes
Ce rapport fournit une liste détaillée de tous les utilisateurs ainsi que leurs appartenances aux groupes associées. Sur la base de ces affiliations, il met en évidence les droits d'accès VPN effectifs que les utilisateurs héritent via les groupes attribués.
Cela permet d'identifier qui a accès aux ressources VPN, de vérifier les droits appropriés et de détecter d'éventuels comptes disposant de privilèges excessifs résultant d'autorisations basées sur des groupes.

Vue d'ensemble de l'appartenance des utilisateurs et des groupes

All LDAP Users
-est membre du groupe : Trusted Users
-est membre du groupe : SSLVPN Services
-est membre du groupe : LAN Access66
- Accorde des droits d'accès à :WAN Primary IP
- Accorde des droits d'accès à :LAN Primary Subnet
- Accorde des droits d'accès à :WAN-GoogleDNS-8.8.8.8
Isabel
-est membre du groupe : Trusted Users
-est membre du groupe : Content Filtering Bypass
-est membre du groupe : Limited Administrators
LocalAdmin
-est membre du groupe : Trusted Users
-est membre du groupe : SonicWALL Administrators
Robert
-est membre du groupe : Trusted Users
-est membre du groupe : Guest Administrators
Sylvia
-est membre du groupe : Trusted Users
-est membre du groupe : Guest Administrators
UDS-SNWL-Admins@uds.local
-est membre du groupe : SonicWALL Administrators
Udo
-est membre du groupe : Trusted Users
-est membre du groupe : SonicWALL Read-Only Admins
Uwe
-est membre du groupe : Trusted Users
-est membre du groupe : SonicWALL Administrators
-est membre du groupe : SSLVPN Services
-est membre du groupe : LAN Access66
- Accorde des droits d'accès à :WAN Primary IP
- Accorde des droits d'accès à :LAN Primary Subnet
- Accorde des droits d'accès à :WAN-GoogleDNS-8.8.8.8
Webadmin
-est membre du groupe : Trusted Users
-est membre du groupe : SonicWALL Administrators
-est membre du groupe : SSLVPN Services
apiuser
-est membre du groupe : Trusted Users
-est membre du groupe : SonicWALL Administrators
mschmitz
-est membre du groupe : Trusted Users
-est membre du groupe : SonicWALL Administrators
-est membre du groupe : SSLVPN Services
-est membre du groupe : LAN Access66
- Accorde des droits d'accès à :WAN Primary IP
- Accorde des droits d'accès à :LAN Primary Subnet

Vue d'ensemble de l'appartenance des utilisateurs et des groupes

mschmitz (suite)

- Accorde des droits d'accès à :WAN-GoogleDNS-8.8.8.8

Annuaires d'utilisateurs externes

Informations complémentaires

Lorsque le nombre de comptes utilisateurs locaux sur un pare-feu dépasse un seuil restreint (généralement autour de 10 utilisateurs), la gestion des identités directement sur le pare-feu devient inefficace, sujette aux erreurs et difficile à faire évoluer. Dans de tels environnements, il est fortement recommandé d'intégrer un annuaire d'utilisateurs externe tel que LDAP, RADIUS ou TACACS+.

1. Gestion centralisée des utilisateurs
Les annuaires d'utilisateurs externes fournissent une source unique et fiable pour les identités des utilisateurs.
- Les comptes utilisateurs sont créés, modifiés et supprimés dans un système central unique.
- Les modifications telles que les mises à jour de mots de passe ou la désactivation de comptes s'appliquent immédiatement à tous les systèmes connectés.
- L'effort administratif est considérablement réduit par rapport à la gestion individuelle des utilisateurs sur chaque pare-feu.

Cela devient de plus en plus important à mesure que le nombre d'utilisateurs augmente et que les changements de personnel se produisent plus fréquemment.

2. Sécurité améliorée et risque réduit
La gestion d'un nombre croissant d'utilisateurs locaux du pare-feu augmente au fil du temps le risque de failles de sécurité.
- Des comptes orphelins peuvent rester actifs après le départ d'employés de l'organisation.
- Les politiques de mots de passe peuvent être incohérentes ou appliquées de manière non uniforme.
- La gestion manuelle des utilisateurs augmente la probabilité d'erreurs de configuration.

Les systèmes d'authentification externes appliquent des politiques de sécurité cohérentes, notamment la complexité des mots de passe, la rotation des mots de passe, les règles de verrouillage de compte et, lorsque cela est pris en charge, l'authentification multifacteur.

3. Meilleure évolutivité et maintenabilité à long terme
Les pare-feu sont conçus principalement pour l'inspection du trafic et l'application des politiques, et non pour la gestion du cycle de vie des identités.
- Gérer un petit nombre d'utilisateurs locaux peut être acceptable.
- Au-delà d'environ 10 utilisateurs, la charge administrative augmente de manière disproportionnée.
- Les annuaires externes s'adaptent à des dizaines, des centaines ou des milliers d'utilisateurs sans augmenter la complexité sur le pare-feu.

Le pare-feu devient un consommateur de services d'identité plutôt que le propriétaire des données utilisateur.

4. Contrôle d'accès basé sur les rôles (RBAC)
Les annuaires d'utilisateurs externes permettent d'attribuer des droits d'accès à l'aide de groupes plutôt que de comptes utilisateurs individuels.
- Les utilisateurs sont affectés à des groupes d'annuaire tels que les utilisateurs VPN ou les administrateurs de pare-feu.
- Les règles de pare-feu font référence à ces groupes plutôt qu'à des utilisateurs spécifiques.
- Les modifications d'accès peuvent être mises en œuvre sans modifier la configuration du pare-feu.

Cette séparation entre la gestion des identités et l'autorisation améliore la clarté, la cohérence et l'efficacité opérationnelle.

5. Audit et conformité facilités
Les normes de sécurité et les politiques internes exigent souvent une traçabilité claire de l'accès des utilisateurs.
Les systèmes d'authentification externes fournissent des journaux d'authentification centralisés, des événements de connexion traçables et une responsabilisation claire par utilisateur.

Cela simplifie considérablement les audits et soutient la conformité avec des cadres tels que l'ISO 27001, le NIST ou les exigences de gouvernance interne.

6. Intégration transparente avec l'infrastructure existante
La plupart des organisations exploitent déjà des systèmes d'identité centralisés.
- LDAP ou Active Directory pour les identités utilisateur
- RADIUS pour l'accès VPN et réseau
- TACACS+ pour le contrôle d'accès administratif

Intégrer le pare-feu à ces systèmes évite les bases de données utilisateur en double et aligne l'accès au pare-feu sur les processus informatiques établis.

7. Réduction des erreurs opérationnelles
La gestion manuelle des utilisateurs sur les pare-feu entraîne fréquemment des problèmes opérationnels.

- Suppressions de comptes oubliées
- Autorisations incohérentes
- Dérive de configuration au fil du temps

Déléguer l'authentification à un système externe permet d'obtenir des configurations de pare-feu plus propres et de réduire le risque d'erreur humaine.

Conclusion
Bien que les utilisateurs locaux du pare-feu puissent suffire pour de très petits environnements, ils n'évoluent pas efficacement. Une fois que le nombre d'utilisateurs dépasse environ 10, l'utilisation d'un annuaire d'utilisateurs externe offre des avantages clairs en termes de sécurité, d'évolutivité, d'efficacité administrative et d'auditabilité.

Pour les environnements moyens et grands, l'intégration de LDAP, RADIUS ou TACACS+ est considérée comme une bonne pratique et une exigence fondamentale pour des opérations de pare-feu durables et sécurisées.

Rapport des zones

Explication

Ce rapport montre les détails concernant les zones

Rapport des zones

Zone	Type	Member Interfaces	Trust	Active Security Services	SSLVPN	SSO
060466	1	None	Blocked	GAV, IPS, ASPY	No	No
150971-Test	1	None	Blocked	None	No	No
DMZ	2	None	Allowed	None	No	Yes
DMZ-sec	2	X3, X7	Blocked	None	No	Yes
DMZ-unsec	2	X2	Blocked	None	No	No
LAN	1	X0, X6, X6:V100	Allowed	GAV, IPS, ASPY, DPI-SSL-C	No	Yes
MULTICAST	6	None	Blocked	None	No	No
SSLVPN	8	None	Blocked	None	Yes	No
Test	1	None	Blocked	GAV, IPS, ASPY, DPI-SSL-C	No	Yes
VPN	5	None	Blocked	None	No	No
WAN	0	X1, X5	Blocked	GAV, IPS, ASPY, DPI-SSL-S, GVPN	Yes	No

Nombre d'enregistrements : 11

Rapport de maintenance

Explication

Le rapport de maintenance aide à identifier les éléments de configuration qui devraient être examinés régulièrement afin de maintenir le pare-feu propre, efficace et facile à gérer. Au fil du temps, les configurations de pare-feu s'accroissent naturellement à mesure que de nouvelles règles, objets, VPN et services sont ajoutés. Sans maintenance périodique, des entrées obsolètes ou inutilisées peuvent s'accumuler, augmentant la charge administrative et compliquant le dépannage.
Ce rapport met en évidence les éléments de configuration susceptibles de nécessiter une attention particulière, tels que les règles de pare-feu désactivées ou inutilisées, les politiques NAT inactives, les objets d'adresse et de service inutilisés, les services de sécurité expirés et d'autres éléments de configuration qui ne sont plus activement utilisés. Il identifie également les paramètres pouvant bénéficier d'une optimisation ou d'un nettoyage.
L'objectif de ce rapport n'est pas de recommander la suppression automatique de chaque élément répertorié. Il fournit plutôt aux administrateurs une vue d'ensemble structurée des composants de configuration devant être vérifiés avant toute modification. Certains objets ou règles peuvent encore être nécessaires pour des projets futurs, des environnements temporaires, des procédures de reprise après sinistre ou des services rarement utilisés.
Une maintenance régulière offre plusieurs avantages importants :
- Réduit la complexité de la configuration et améliore la lisibilité.
- Facilite considérablement le dépannage et les audits.
- Aide à identifier les éléments de configuration obsolètes ou oubliés.
- Réduit le risque d'erreurs de configuration accidentelles.
- Améliore la gérabilité à long terme du pare-feu.
- Soutient un environnement de sécurité bien documenté et entretenu de manière professionnelle.
Un pare-feu bien entretenu est plus facile à administrer, plus facile à auditer, et constitue une base plus solide pour les futures modifications de configuration et améliorations de sécurité.

Conventions de nommage des objets d’adresse

Explication

Importance des conventions de nommage communes pour les objets d'adresse
Une gestion efficace des objets d'adresse du pare-feu est essentielle pour maintenir un environnement réseau sécurisé et bien organisé. L'utilisation de conventions de nommage cohérentes et significatives est un facteur clé contribuant à cette efficacité.

Clarté et administration plus rapide
Lorsque les objets d'adresse suivent des normes de nommage uniformes, les administrateurs peuvent immédiatement en reconnaître l'objectif, l'emplacement ou le service associé sans avoir à consulter des données de configuration détaillées. Cela réduit le temps consacré au dépannage, à la mise à jour des règles ou aux modifications de politiques, et minimise le risque de modifier le mauvais objet.

Cohérence et précision de la configuration
Des formats de nommage standardisés établissent une uniformité dans toutes les configurations. Cela évite les doublons, prévient la confusion et réduit les erreurs de configuration susceptibles d'entraîner des autorisations d'accès indésirables ou des flux de communication bloqués. Des noms prévisibles permettent aux administrateurs d'interpréter les politiques de pare-feu de manière plus efficace et précise.

Meilleure collaboration et transfert de connaissances
Des conventions de nommage cohérentes permettent aux équipes de travailler avec une compréhension partagée. Les administrateurs qui ne connaissent pas une configuration peuvent néanmoins interpréter immédiatement l'utilisation des objets et leurs dépendances. Cela améliore la collaboration, simplifie l'intégration de nouveau personnel et garantit la continuité dans le temps, même en cas de changement de responsabilités.

Conclusion
Des conventions de nommage communes renforcent la maintenabilité, la précision et la transparence des configurations de pare-feu. En améliorant la clarté, en réduisant la complexité de la configuration et en favorisant la collaboration, elles contribuent de manière significative à une administration réseau sécurisée et durable.

Conventions de nommage des objets d’adresse

Address Object Name old	Address Object Name new
SSLVPN-NetExtender Range	AO-SSLVPN-NetExtender Range-192.168.168.100
WAN-GoogleDNS-8.8.8.8	AO-WAN-GoogleDNS-8.8.8.8
WAN-TZ570-10.10.10.254	AO-WAN-TZ570-10.10.10.254
LAN-UDS-Analytics-10.100.10.50	AO-LAN-UDSAnalytics-10.100.10.50
WAN-GoogleDNS-8.8.8.8-2	AO-WAN-GoogleDNS2-8.8.8.8
TZ570 LAN	AO-VPN-TZ570 LAN-10.10.10.0
Server	AO-LAN-Server-10.99.10.223
MartinSchmitz	AO-LAN-MartinSchmitz-1.1.1.1
KlausMeier	AO-LAN-KlausMeier-1.1.2.2
FTP Server Private	AO-LAN-FTP Server Private-172.20.20.101
FTP Server Public1	AO-WAN-FTP Server Public1-10.10.20.2
Test	AO-LAN-Test-10.100.10.99
Test1	AO-LAN-Test1-10.100.10.99
Test4	AO-LAN-Test4-10.100.10.99
x0 und x6 subnet	AO--x0 und x6 subnet-0.0.0.0
Test12	AO-LAN-Test12-10.100.10.99
Test_111	AO-LAN-Test_111-10.100.10.111
Test_112	AO-LAN-Test_112-10.100.10.112
Test_113	AO-LAN-Test_113-10.100.10.113
Test_114	AO-LAN-Test_114-10.100.10.114
Test_115	AO-LAN-Test_115-10.100.10.115
Test_116	AO-LAN-Test_116-10.100.10.116
Test_117	AO-LAN-Test_117-10.100.10.117
Test_118	AO-LAN-Test_118-10.100.10.118
Test13	AO-LAN-Test13-10.100.10.13
Syslog Synology	AO-WAN-Syslog Synology-10.10.40.50
Test Group	AO--Test Group-0.0.0.0

Objets d'adresse en double

Explication

Analyse des objets d'adresse en double
Les objets d'adresse en double - où des noms différents font référence à la même adresse IP ou au même réseau - peuvent engendrer de multiples défis opérationnels et sécuritaires sur les pare-feu.
1. Complexité accrue et risque d'erreur de configuration
Lorsque plusieurs objets font référence à la même destination, les administrateurs peuvent ne pas savoir lequel utiliser. Cela complique la création des politiques, augmente la probabilité d'utiliser le mauvais objet et ralentit les audits, le dépannage et les processus de changement.
2. Politiques conflictuelles ou se chevauchant
Différents objets représentant la même IP peuvent être utilisés de manière incohérente selon les règles. Une règle peut autoriser le trafic tandis qu'une autre le bloque, entraînant un comportement imprévisible et une analyse des politiques difficile.
3. Application incohérente de la sécurité
Lorsque différentes équipes ou différents administrateurs créent des objets distincts pour la même ressource, l'application des politiques devient fragmentée. Cela peut entraîner un accès involontaire ou une couverture partielle des politiques, affaiblissant la posture de sécurité globale.
4. Effort de maintenance accru
Toute modification affectant un objet dupliqué doit être mise à jour dans toutes les références de politiques. Oublier un emplacement peut entraîner des règles obsolètes, des lacunes dans les restrictions d'accès ou une dérive de configuration.
Bonnes pratiques recommandées
– *Consolider les objets d'adresse :* identifier les entrées en double et les remplacer par un seul objet représentant chaque IP, sous-réseau ou ressource.
– *Utiliser des conventions de nommage claires :* les noms doivent refléter l'objectif ou l'identité de la ressource, améliorant ainsi la cohérence et la lisibilité.
– *Effectuer des audits réguliers :* un nettoyage périodique réduit la redondance et améliore la qualité des politiques.
– *Documenter l'utilisation et la propriété :* une documentation adéquate facilite la maintenance et évite la recréation d'objets inutiles.

Le nettoyage des objets d'adresse en double améliore la clarté des règles, simplifie l'administration des politiques, réduit les erreurs opérationnelles et contribue à une configuration de sécurité plus solide et plus prévisible.

Duplicate Address Objects

IP	Name
- aucun enregistrement trouvé -	

Journalisation externe

Explication

La journalisation/télémétrie externe sur un pare-feu (par exemple Syslog, IPFIX/NetFlow, traps SNMP) est importante car le pare-feu est l'un des rares appareils capables d'observer de manière fiable qui a communiqué avec qui, quand, comment, et ce qui a été bloqué ou autorisé. Sans exporter ces signaux, vous opérez essentiellement à l'aveugle : vous pouvez toujours être protégé par la politique, mais vous perdez la capacité de détecter, d'enquêter et de prouver ce qui s'est passé.
D'un point de vue sécurité, les journaux externes constituent la base de la détection et de la réponse aux incidents. Les attaques s'annoncent rarement par une seule alarme évidente. Elles apparaissent sous forme de schémas - échecs de connexion répétés, anomalies VPN, correspondances de politiques, connexions sortantes inattendues, mouvement latéral ou trafic vers des destinations suspectes. Un SIEM ou une plateforme de journalisation peut corréler ces schémas entre plusieurs sources (pare-feu + terminaux + identité + serveurs). Les événements du pare-feu fournissent souvent le premier indicateur de haute qualité qu'un problème existe, et la télémétrie de flux (NetFlow/IPFIX) fournit le « récit réseau » nécessaire pour comprendre l'étendue et l'impact.
La collecte externe est également essentielle pour la criminalistique et la responsabilisation. Les pare-feu disposent d'une conservation locale limitée des journaux et peuvent perdre des données lors de redémarrages, de mises à jour ou de rotations de stockage. La journalisation centralisée préserve les preuves sur des périodes plus longues, soutient les exigences légales/réglementaires et permet des rapports fiables. En pratique, de nombreuses enquêtes commencent des jours ou des semaines après la compromission initiale. Si les journaux n'étaient conservés que localement, la période clé pourrait déjà avoir disparu.
Sur le plan opérationnel, la télémétrie améliore la stabilité et le dépannage. La surveillance SNMP et les traps fournissent des alertes précoces sur la pression CPU/mémoire, les erreurs d'interface, l'instabilité des tunnels ou la saturation des ressources - des problèmes qui peuvent ressembler à des « pannes aléatoires » à moins de disposer de données en série temporelle. Les enregistrements de flux aident à valider l'utilisation de la bande passante, à identifier les principaux générateurs de trafic, à détecter les erreurs de configuration (par exemple, le routage asymétrique) et à confirmer si un changement de politique a réellement eu l'effet escompté.
Enfin, la journalisation/télémétrie externe favorise l'amélioration continue. Elle permet de mesurer l'efficacité des politiques, d'ajuster les règles trop permissives ou trop bruyantes, et d'identifier le Shadow IT ou les services risqués. En bref : exporter les journaux et la télémétrie du pare-feu transforme le pare-feu d'une boîte qui « bloque le trafic » en un contrôle que vous pouvez vérifier, auditer et rendre opérationnel - ce qui fait toute la différence entre disposer de contrôles de sécurité et disposer d'une assurance de sécurité.

Journalisation externe

Central Management	
Central Management (NSM / GMS):	off
NSM ZeroTouch:	enabled

Syslog	
Syslog Server Name:	n/a
Syslog Standby Server Name:	n/a
Syslog Server Port:	n/a

Netflow	
Netflow Internal:	n/a
Netflow External:	n/a
Netflow External Address:	n/a

Log to FTP Server	
Log to FTP Server:	
FTP Server IP Address:	n/a

Règles de pare-feu désactivées

Explication

Importance des règles de pare-feu désactivées
Les règles de pare-feu désactivées, bien qu'elles n'appliquent pas activement de contrôles de sécurité, restent pertinentes au sein de la configuration du pare-feu et de la stratégie de sécurité globale.
Sauvegarde opérationnelle et réactivation rapide
Les règles désactivées servent souvent d'alternatives de configuration prédéfinies. Les administrateurs peuvent désactiver temporairement une règle pendant la maintenance, le dépannage ou des modifications planifiées, puis la réactiver plus tard sans avoir à repenser ou recréer la politique. Cela garantit une restauration rapide des contrôles de sécurité prévus.
Documentation de configuration et d'audit
Les règles inactives donnent un aperçu des ensembles de règles historiques et des décisions de sécurité antérieures. Les garder visibles favorise les audits, la vérification de conformité et l'analyse forensique en préservant l'intention de configuration et l'historique des modifications.
Flexibilité pour les besoins futurs
À mesure que les environnements réseau évoluent, des règles précédemment désactivées peuvent redevenir pertinentes. Les conserver permet une réactivation ou une modification rapide sans avoir à recréer des politiques d'accès complexes ou des objets d'adresse à partir de zéro.
Conclusion
Bien que les règles de pare-feu désactivées ne filtrent pas activement le trafic, elles restent des points de référence utiles pour la récupération opérationnelle, la documentation des configurations antérieures et l'adaptation rapide aux futurs besoins de sécurité. Elles doivent être révisées périodiquement pour s'assurer qu'elles restent valides, intentionnelles et alignées sur les objectifs de sécurité actuels.

Règles de pare-feu désactivées

Ena	A	Name	SrcZone	DstZone	SrcNet	DstNet	SrcSvc	DstSvc

- aucun enregistrement trouvé -

Nombre d'enregistrements : 0

Règles de pare-feu non utilisées depuis longtemps (IPv4)

Explication

Règles de pare-feu non utilisées depuis une période prolongée
Les règles de pare-feu qui n'ont pas été utilisées pendant une longue période indiquent souvent des voies d'accès obsolètes, des services mis hors service ou des configurations héritées qui ne sont plus pertinentes. Conserver des règles inutilisées augmente la charge administrative et peut créer une exposition de sécurité inutile.

Les règles inactives peuvent être réactivées ou modifiées par erreur, accordant potentiellement un accès non intentionnel ou affaiblissant l'application des politiques. Supprimer ou désactiver ces règles aide à maintenir une base de règles propre, améliore la gérabilité et réduit la surface d'attaque globale de l'environnement.

Une révision régulière des règles inutilisées garantit que seules les voies d'accès nécessaires et activement utilisées subsistent, favorisant à la fois l'efficacité opérationnelle et les bonnes pratiques de sécurité.

Le rapport suivant montre les règles non utilisées depuis plus de 365 jours.

Règles de pare-feu non utilisées depuis longtemps (IPv4)

Ena	A	Name	SrcZone	DstZone	SrcNet	DstNet	SrcSvc	DstSvc	Last time hit
YES	A	Allow WAN1	LAN	WAN	KlausMeier	any	any	any	Règles de pare-feu no...
YES	A	Heating Maintenance	WAN	LAN	any	LAN Subnets	any	SSH	Règles de pare-feu no...
YES	A	Test 24	WAN	060466	any	any	any	OSPF	Règles de pare-feu no...
YES	A	Test 25	WAN	060466	any	any	any	POP3 (Retrieve E-Mail)	Règles de pare-feu no...
YES	A	Test 23	WAN	060466	any	any	any	MSN	Règles de pare-feu no...
YES	A	Allow WAN1	DMZ-unsec	WAN	any	any	Citrix UDP	any	Règles de pare-feu no...
YES	A	Allow syslog	DMZ-unsec	DMZ-unsec	any	any	SSH Management	any	Règles de pare-feu no...
YES	A	Test 22	DMZ-unsec	DMZ-sec	any	any	any	MSN	Règles de pare-feu no...
YES	A	Complicated Rule	DMZ-unsec	Test	any	any	Citrix UDP	any	Règles de pare-feu no...
YES	A	Allow WAN1	DMZ-sec	WAN	any	any	Enhanced TV	any	Règles de pare-feu no...
YES	A	My Rule	DMZ-sec	DMZ-unsec	any	any	any	FTP Data	Règles de pare-feu no...
YES	A	Test 17	DMZ-sec	DMZ-unsec	any	any	any	HTTPS	Règles de pare-feu no...
YES	A	Test 20	DMZ-sec	DMZ-unsec	any	any	any	Kazaa / FastTrack	Règles de pare-feu no...
YES	A	Test 21	DMZ-sec	DMZ-unsec	any	any	any	Lotus Notes	Règles de pare-feu no...
YES	A	Test 19	DMZ-sec	DMZ-unsec	any	any	any	IKE	Règles de pare-feu no...
YES	A	Test 18	DMZ-sec	DMZ-unsec	any	any	any	ICMP	Règles de pare-feu no...
YES	A	Rule6	DMZ-sec	Test	any	Test13	Citrix TCP	any	Règles de pare-feu no...
YES	A	Rule10	DMZ-sec	Test	WAN-GoogleDNS-8.8.8.8	any	Direct Connect	any	Règles de pare-feu no...
YES	A	Allow Citrix	any		any	any	Citrix UDP	any	Règles de pare-feu no...
YES	A	Allow FTP	any		any	any	FTP	any	Règles de pare-feu no...
YES	A	Allow management via ...	SSLVPN	LAN	SSLVPN-NetExtender Range	any	any	HTTPS Management	2025-03-31 11:40:59

- Les règles ajoutées automatiquement sont exclues de ce rapport

Nombre d'enregistrements : 21

Politiques NAT (traduction d'adresses réseau) désactivées (IPv4)

Explication

Politiques NAT désactivées et leur impact
Les politiques NAT (traduction d'adresses réseau) désactivées sur les pare-feu peuvent engendrer des problèmes opérationnels et de sécurité importants au sein d'un réseau. Voici un aperçu des principaux risques et implications techniques associés aux règles NAT inactives ou supprimées.

1. Perte de segmentation réseau
Les politiques NAT favorisent la séparation logique entre réseaux internes et externes en traduisant les adresses IP internes avant que le trafic ne quitte le réseau.
Risques potentiels :
– *Exposition des IP internes :* sans NAT, les schémas d'adressage internes peuvent devenir visibles de l'extérieur, rendant accessibles des appareils auparavant isolés.
– *Isolation réduite entre les zones :* le NAT favorise l'isolation entre les segments LAN, DMZ et WAN. Un NAT désactivé peut involontairement brouiller les limites de sécurité.

2. Risques de sécurité accrus
Le NAT fournit indirectement une couche de sécurité en empêchant les connexions entrantes non sollicitées vers les hôtes internes.
Conséquences possibles :
– Les attaquants peuvent cibler directement les appareils internes
– Les restrictions basées sur le pare-feu peuvent être contournées
– Les ressources internes deviennent plus faciles à énumérer ou à scanner

3. Interruptions de communication
De nombreux flux de communication réseau supposent que le NAT est actif pour la traduction et le routage.
Lorsque le NAT est désactivé :
– Les appareils peuvent perdre l'accès aux services externes
– Les utilisateurs peuvent rencontrer une connectivité incohérente
– Le dépannage devient plus complexe en raison de défaillances de routage ou de services inaccessibles

4. Problèmes de connectivité multi-réseaux et VPN
Les VPN, le routage et les technologies d'accès à distance dépendent souvent du NAT pour aligner les espaces d'adresses internes et externes.
Risques clés :
– Les sessions d'accès à distance peuvent échouer
– Un chevauchement réseau peut survenir en cas de conflit d'espaces IP
– Les systèmes externes ne peuvent pas router correctement le trafic retour

5. Défis d'application des politiques et de surveillance
La logique de contrôle d'accès s'appuie fréquemment sur le NAT pour suivre et catégoriser les flux.
Conséquences d'un NAT désactivé :
– Capacité réduite à surveiller ou corréler le trafic
– Difficulté à attribuer une activité à des appareils/utilisateurs spécifiques
– Lacunes dans la précision de la journalisation

6. Consommation accrue d'espace IP public
Le NAT permet à de nombreux appareils internes de partager une ou un petit pool d'adresses IP publiques.
Sans NAT :
– Chaque système peut nécessiter sa propre IP routable
– L'épuisement des IPv4 devient une préoccupation opérationnelle réelle

Conclusion
Les politiques NAT désactivées peuvent provoquer des défaillances de routage inattendues, des limites de protection affaiblies et une exposition accrue à des risques de sécurité. Dans la plupart des environnements, le NAT sert non seulement à la traduction d'adresses mais aussi de méthode pour appliquer l'isolation, la visibilité de journalisation et un comportement de routage prévisible. Pour des opérations stables et sécurisées, les politiques NAT doivent être soigneusement révisées, correctement maintenues et désactivées uniquement dans des scénarios de conception intentionnels et bien contrôlés.

- Les règles ajoutées automatiquement sont exclues de ce rapport

Politiques NAT (traduction d'adresses réseau) désactivées (IPv4)

Ena	Name	Original Source	Translated Source	Original Destination	Translated Destination	Original Service	Translated Service
NO	Test disabled NAT	DMZ-sec Subnets	Original	Any	Server	Citrix UDP	Original
NO	My Rule	DMZ-unsec Subnets	Original	All WAN IP	DEAG_Test	Any	Original
NO	Deact 3	FTP Server Private	FTP Server Public1	Any	Original	Any	Original

Politiques NAT activées et sans correspondance (IPv4)

Explication

Politiques NAT sans correspondance de trafic
Ce rapport met en évidence les politiques NAT (traduction d'adresses réseau) actuellement activées mais non utilisées pendant la période surveillée. Une politique NAT sans correspondance enregistrée indique généralement que la règle ne correspond plus à des flux de trafic actifs ou est associée à des services, réseaux ou appareils qui ne sont plus utilisés.

Causes possibles des politiques NAT inutilisées
– Le service correspondant n'est plus actif
– Une référence d'appareil ou de réseau a changé
– Le routage a été repensé, rendant cette traduction NAT obsolète
– Une règle temporaire ou liée à une migration n'a jamais été supprimée

Pourquoi les politiques NAT inutilisées sont importantes
1. Complexité accrue des politiques
Les entrées NAT inutilisées rendent la configuration plus difficile à comprendre et à maintenir. Les administrateurs peuvent consacrer du temps supplémentaire à évaluer des règles qui ne sont plus pertinentes, ralentissant le dépannage et la gestion des changements.

2. Risque d'activation accidentelle
Une politique NAT dormante peut devenir active si les conditions réseau changent ou si le routage évolue. Cela pourrait exposer par inadvertance des appareils internes, modifier les correspondances d'adresses ou contourner les politiques d'accès prévues.

3. Exposition potentielle à des risques de sécurité
Même inutilisée, une règle NAT définit toujours un chemin de traduction possible. Si elle est activée par inadvertance, elle peut :
– révéler l'adressage interne
– permettre des connexions entrantes ou sortantes indésirables
– contourner les points de filtrage ou d'inspection attendus

4. Efficacité opérationnelle réduite
Les grands ensembles de règles NAT augmentent la charge de travail administrative et réduisent la clarté de la configuration. La suppression des entrées obsolètes permet d'obtenir un ensemble de politiques plus clair et plus prévisible, et réduit le risque opérationnel.

Bonnes pratiques de maintenance recommandées
– Vérifier périodiquement si les règles NAT sont toujours nécessaires
– Documenter la propriété et l'objectif prévu des règles
– Supprimer les correspondances inutilisées ou les désactiver temporairement pour validation
– Revoir les politiques NAT après des refontes de réseau, des migrations ou des activités de mise hors service

Conclusion
Les politiques NAT activées sans activité de trafic indiquent souvent des objets de configuration obsolètes ou inutiles. Le nettoyage des règles inutilisées réduit la complexité, prévient les chemins d'exposition non intentionnels et améliore la maintenabilité ainsi que la posture de sécurité. Une révision régulière garantit que la politique du pare-feu reflète fidèlement le comportement réseau requis et actif.

- Les règles ajoutées automatiquement sont exclues de ce rapport

Politiques NAT activées et sans correspondance (IPv4)

Ena	Name	Original Source	Translated Source	Original Destination	Translated Destination	Original Service	Translated Service
NO	Test disabled NAT	DMZ-sec Subnets	Original	Any	Server	Citrix UDP	Original
YES	Test 1	DMZ-sec Subnets	Original	Any	CSE_Access_Tier_AIP_1	Citrix TCP	Original
NO	My Rule	DMZ-unsec Subnets	Original	All WAN IP	DEAG_Test	Any	Original
NO	Deact 3	FTP Server Private	FTP Server Public1	Any	Original	Any	Original
YES	Default NAT Policy	Any	Any	Any	Any	Any	Original

Paramètres WAN MTU

Explication

Cette section vérifie si le paramètre WAN MTU du pare-feu SonicWall est configuré de manière inhabituellement basse.
Une valeur MTU trop basse peut réduire l'efficacité de la transmission et affecter négativement les performances réseau.
Si un tel paramètre est détecté, il doit être examiné pour confirmer qu'il est techniquement nécessaire et non le résultat d'une limitation de configuration inutile.

X1	WAN	1500	ok	-
X5	WAN	1500	ok	-