

Microsoft ISA Server 2000 Standard Edition – Guide d'installation et de déploiement

Sommaire

- I [À propos de ce guide](#)
- I [Introduction](#)
- I [Considérations sur la planification](#)
- I [Installation de ISA Server](#)
- I [Migration à partir de Microsoft Proxy Server 2.0](#)
- I [Mise à niveau vers ISA Server Enterprise Edition](#)
- I [Installation et configuration clientes](#)
- I [Scénarios de déploiement](#)

À propos de ce guide

Internet offre aux entreprises de nouvelles possibilités de connexion avec leurs clients, partenaires et employés. Tout en présentant de formidables opportunités, Internet introduit également de nouveaux risques et de nouveaux problèmes dans les domaines de la sécurité, des performances et de la gestion. Microsoft [Internet Security and Acceleration \(ISA\) Server](#) répond aux besoins des entreprises d'aujourd'hui travaillant avec Internet. ISA Server offre un pare-feu multicouche qui contribue à la protection de vos ressources réseau. Le cache Web de Microsoft ISA Server permet aux entreprises d'économiser de la bande passante et fournit un accès Web plus rapide aux utilisateurs en mettant à disposition les objets à partir d'une source locale, plutôt que par l'intermédiaire d'un réseau Internet régulièrement surchargé.

Qu'il soit déployé sous la forme de composants dédiés ou en tant que pare-feu et serveur cache intégré, ISA Server propose une console de gestion unifiée qui simplifie la gestion de la sécurité et des accès. Conçu pour la plate-forme [Windows 2000](#), ISA Server offre une connectivité à Internet rapide et sécurisée, alliée à de puissants outils de gestion intégrés.

ISA Server représente un apport précieux pour les responsables informatiques, les administrateurs réseau et les responsables de la sécurité de l'information dans les entreprises de toutes tailles, soucieuses de la sécurité, des performances, de la facilité de gestion et des coûts d'exploitation de leurs réseaux. ISA Server peut être utilisé dans une grande diversité d'organisations, des petites entreprises et succursales aux fournisseurs de services Internet (ISP) et entreprises d'hébergement sur le Web, ainsi qu'aux sites de commerce électronique.

À qui s'adresse ce guide ?

Ce guide s'adresse aux responsables système, aux administrateurs réseau et aux utilisateurs avec pouvoir dans les petites entreprises souhaitant apprendre à installer et déployer ISA Server sur leur réseau. Il part du principe que vous connaissez les concepts de base de la mise en réseau, y compris DNS, DHCP, Routage et accès distant, les réseaux TCP/IP (Transmission Control Protocol/Internet Protocol) et autres composants réseau de Windows 2000.

Objectif de ce guide

Ce guide offre une vue d'ensemble de Microsoft ISA Server et fournit les informations de base dont vous avez besoin pour planifier sa mise en œuvre.

Vous y trouverez des procédures d'installation détaillées, des listes de contrôle pour la configuration après l'installation et des scénarios précis suggérant des exemples d'utilisation de ISA Server sur votre réseau.

Introduction

Ce chapitre offre une vue d'ensemble de Microsoft Internet Security and Acceleration (ISA) Server. Il décrit également des scénarios courants d'utilisation de Microsoft ISA Server sur le réseau.

Ce chapitre se compose des sections suivantes :

- I Présentation de Microsoft ISA Server
- I Fonctionnalités et scénarios d'utilisation

Présentation de Microsoft ISA Server

Face à l'explosion des activités commerciales basées sur Internet et au nombre considérable de réseaux d'entreprise qui y sont connectés, il est plus que jamais nécessaire de disposer d'une passerelle puissante et facile à administrer qui fournisse une connexion sécurisée tout en augmentant et améliorant les performances réseau. ISA Server répond à ces besoins en proposant une solution complète de connectivité Internet comprenant à la fois un pare-feu et une solution de cache Web complète. Ces services sont complémentaires : vous pouvez utiliser l'une de ces fonctionnalités ou les deux, lorsque vous installez ISA Server sur votre réseau.

ISA Server vous permet de mettre en œuvre votre stratégie de sécurité d'entreprise en configurant un large ensemble de règles qui spécifient les sites, les protocoles et les contenus qui peuvent transiter par ISA Server. ISA Server surveille les échanges de demandes et de réponses entre Internet et les ordinateurs clients internes, contrôlant qui est habilité à accéder à quels ordinateurs du réseau de l'entreprise. Il contrôle également les ordinateurs sur Internet auxquels les clients internes peuvent accéder.

ISA Server offre de nombreuses options de sécurité, y compris le filtrage des paquets et le blocage des intrus. Vous pouvez créer des stratégies d'accès basées sur des informations au niveau de l'utilisateur ou des adresses IP (Internet Protocol) et déterminer les cas dans lesquels la règle doit être appliquée.

ISA Server permet la publication sécurisée. Vous pouvez utiliser ISA Server pour définir une stratégie de publication qui protège les serveurs de publication internes et les rend accessibles aux clients Internet en toute sécurité.

ISA Server implémente un cache d'objets fréquemment demandés. Vous pouvez configurer le cache pour vous assurer qu'il contient les données les plus fréquemment utilisées par l'organisation ou les plus souvent sollicitées par vos clients Internet.

ISA Server est extensible. ISA Management possède une interface COM correspondante que les administrateurs peuvent programmer à l'aide de langages de programmation ou de scripts de haut niveau. La fonctionnalité centrale du pare-feu peut être étendue par d'autres développeurs, qui mettront en œuvre des filtres d'application ou des filtres Web. La fonctionnalité de cache peut être améliorée grâce à l'interface API (Application Programming Interface). L'interface ISA Management peut être étendue de manière à fournir des utilitaires d'administration intégrés pour les nouvelles extensions.

Fonctionnalités et scénarios d'utilisation

Microsoft a collaboré avec ses clients pour concevoir un produit répondant aux besoins des entreprises Internet d'aujourd'hui : sécurité, performances et facilité de gestion. Les sections suivantes abordent des scénarios utilisateur courants et indiquent comment utiliser les fonctionnalités de ISA Server pour implémenter ces scénarios dans votre réseau.

Connectivité Internet avec un haut niveau de sécurité

ISA Server peut être déployé en tant que pare-feu dédié fonctionnant comme passerelle sécurisée entre l'Internet et les clients internes. En définissant des stratégies d'accès, les administrateurs peuvent empêcher l'accès non autorisé et l'entrée de contenus malintentionnés sur le réseau, et limiter le trafic sortant.

ISA Server vous offre une solution complète de sécurisation de l'accès au réseau, notamment les fonctionnalités de pare-feu et de sécurité répertoriées ci-dessous.

- I **Stratégie d'accès sortant.** Vous pouvez utiliser ISA Server pour configurer des règles de site et de contenu ainsi que des règles de protocole qui contrôlent la façon dont vos clients internes accèdent à Internet. Les règles de site et de contenu spécifient les sites et les contenus accessibles. Les règles de protocole indiquent si un protocole particulier est accessible pour les communications entrantes et sortantes.
- I **Détection d'intrusion.** Les mécanismes intégrés de détection d'intrusion peuvent vous alerter lorsqu'une attaque spécifique est lancée contre votre réseau. Par exemple, vous pouvez configurer l'ordinateur ISA Server pour qu'il vous alerte en cas de détection d'une tentative de balayage de port.
- I **Assistant Sécurité système.** L'Assistant Sécurité de ISA Server vous permet de sécuriser Windows 2000 en définissant le niveau de sécurité approprié à l'aide de modèles prédéfinis.
- I **Filtres d'application.** ISA Server analyse et contrôle le trafic spécifique à une application à l'aide de filtres d'application qui inspectent les données réelles. Vous pouvez activer le filtrage intelligent pour HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), la messagerie électronique, le service de conférence H.323, la diffusion multimédia par flux, l'appel de procédure distantes (RPC), etc.

- I *Prise en charge du réseau privé virtuel (VPN)*. ISA Server comprend un accès distant sécurisé et normalisé aux services de réseau privé virtuel intégré (VPN) de Microsoft Windows 2000.

Accès productif à Internet

L'accès à Internet est désormais un outil fondamental pour tous les professionnels du secteur quaternaire. Étant donné l'importance du trafic Internet transitant par les passerelles réseau, les performances d'accès au Web peuvent se transformer en goulet d'étranglement faisant obstacle à la productivité. Les fonctions de cache Web de ISA Server permettent d'accélérer les accès au Web en mettant en cache les données Internet qui restent ainsi plus facilement accessibles à l'utilisateur. En outre, à l'aide de contrôles d'accès basés sur une stratégie, les administrateurs ont la possibilité de restreindre les sites Web auxquels ont accès certains utilisateurs en fonction de l'heure, du type de données ou d'autres catégories. Grâce à la mise en cache rapide et au contrôle des accès, ISA Server permet de réduire les coûts liés à la gestion des connexions à Internet et d'accroître la productivité des utilisateurs d'Internet. ISA Server utilise la mise en cache en mémoire vive (RAM) ainsi qu'un système efficace d'entrée/sortie des fichiers afin d'accélérer les performances du cache.

Les fonctionnalités de mise en cache de ISA Server sont les suivantes :

- I *Mise en cache hiérarchique*. Microsoft ISA Server vous permet de définir une hiérarchie de caches, en chaînant entre eux les groupes de serveurs ISA, de telle sorte que les clients puissent accéder au cache le plus proche géographiquement ;
- I *Mise en cache inversée*. ISA Server peut mettre en cache le contenu HTTP et FTP des serveurs de publication Web, et améliorer ainsi leur facilité d'accès ;
- I *Mise en cache planifiée*. Vous pouvez utiliser le service de téléchargement du contenu du cache planifié pour configurer le moment où ISA Server doit réactualiser dans son cache le contenu fréquemment demandé sur Internet.

Publication rapide et évolutive, et commerce électronique

Que votre organisation soit spécialisée dans le commerce électronique de détail sur Internet ou qu'il s'agisse d'une grande entreprise cherchant à étendre son champ d'action, Internet est un élément fondamental de sa stratégie. Les entreprises ne peuvent pas se permettre de posséder des sites Web de commerce électronique lents, sans dynamisme, surtout quand la concurrence les talonne à un clic de souris. Le cache Web ISA Server offre aux utilisateurs une navigation rapide sur le Web qui évolue en même temps que votre activité. La mise en cache est également disponible pour les clients Internet demandant des objets présents sur les ordinateurs de votre réseau local.

ISA Server vous permet de publier des services vers Internet sans compromettre la sécurité de votre réseau interne. Vous pouvez configurer des règles de publication Web et de publication serveur qui déterminent les requêtes qui doivent être envoyées en aval vers un serveur placé derrière l'ordinateur ISA Server, afin d'ajouter un niveau de sécurité supplémentaire pour vos serveurs internes.

Vous pouvez utiliser les fonctionnalités suivantes de Microsoft ISA Server pour publier des serveurs.

- I *Publication Web sécurisée*. Les règles de publication Web permettent un accès sécurisé aux serveurs Web internes. Elles autorisent les clients externes à accéder aux serveurs internes tout en protégeant ces derniers contre les accès non autorisés.
- I *Publication sécurisée sur serveurs d'applications*. Les règles de publication de serveur permettent d'accorder à certains clients l'accès aux serveurs internes tout en évitant les tâches fastidieuses de configuration ou d'installation sur le serveur de publication.

ISA Server comporte un Assistant Sécurité du serveur de courrier qui facilite la configuration de Exchange Server sur le réseau local.

Gestion unifiée

La gestion séparée de la sécurité et de la mise en cache nécessite en général de faire appel à des technologies réseau, des équipements d'infrastructure et des administrateurs qualifiés différents, d'où un surcroît de complexité, de coûts et d'incohérences. L'outil administration unifié basé sur une stratégie aide les administrateurs à gérer et sécuriser leur connectivité Internet à partir d'un point central, ce qui réduit la complexité du réseau et le coût global de propriété.

Les entreprises ont généralement tout à gagner à établir des stratégies cohérentes de cache et de pare-feu. L'intégration de la gestion dans ISA Server donne une vue unique de ces stratégies et vous évite de devoir gérer séparément l'infrastructure du cache et du pare-feu.

Considérations sur la planification

Ce chapitre aborde les informations dont vous avez besoin pour planifier et d'éployer Microsoft Internet Security and Acceleration (ISA) Server dans votre entreprise. Il fournit la plupart des informations nécessaires au déploiement de ISA Server dans l'entreprise mais ne prétend pas traiter de tous les aspects réseau.

Le tableau ci-dessous dresse la liste des facteurs à prendre en compte lors de la planification du d'éploiement de ISA Server.

Problème	Description	Voir
De combien d'ordinateurs ai-je besoin ?	La configuration matérielle et la connectivité Internet dépendent de votre mode d'utilisation de ISA Server.	"Conseils pour la planification de la capacité"
De quelles fonctionnalités ISA Server ai-je besoin ?	Vous choisissez les fonctionnalités ISA Server à installer selon les besoins spécifiques à votre réseau.	"Sélection des fonctionnalités ISA Server"
Quels sont les besoins des utilisateurs ?	Déterminez les applications et les services dont vos utilisateurs ont besoin afin de savoir comment configurer les clients.	"Évaluation des besoins des clients"
Dois-je reconfigurer mon réseau ?	Réfléchissez à la façon dont ISA Server va interfonctionner avec votre réseau.	"Considérations sur le réseau existant"

Ce chapitre comprend les sections suivantes :

- I Conseils pour la planification de la capacité
- I Sélection des fonctionnalités ISA Server
- I Évaluation des besoins des clients
- I Interaction avec d'autres services réseau

Conseils pour la planification de la capacité

Pour améliorer les performances, planifiez la configuration matérielle et la connectivité Internet de ISA Server en fonction de la charge prévue. Les sections suivantes décrivent les configurations système recommandées pour différents scénarios d'utilisation.

Configuration minimale requise

ISA Server exige la configuration suivante :

- I Ordinateur personnel avec un processeur à 300 mégahertz (MHz) ou plus, compatible Pentium II
- I Système d'exploitation de l'ordinateur devant être Microsoft Windows 2000 Server avec le Service Pack 1 ou une version supérieure, Microsoft Windows 2000 Advanced Server avec le Service Pack 1 ou une version supérieure, ou Microsoft Windows 2000 Datacenter Server.
- I 256 Mo de mémoire vive
- I 20 Mo d'espace disque disponible
- I Carte réseau compatible avec Windows 2000 pour la communication avec le réseau interne
- I Partition de disque dur local formatée pour le système de fichiers NTFS.

Il est possible d'utiliser jusqu'à quatre processeurs sur l'ordinateur ISA Server. Au-delà, ISA Server ne s'installera pas.

Si vous utilisez ISA Server en mode pare-feu ou intégré, deux cartes réseau sont nécessaires.

Remarque : utilisez toujours le Service Pack le plus récent.

Configuration requise pour une administration à distance

Pour l'administration à distance de ISA Server, il suffit d'installer ISA Management, module exécutable sous Windows 2000 Professionnel ou supérieur.

Une autre solution consiste à installer les services Terminal Server en Mode Administration à distance sur l'ordinateur exécutant ISA Server. Dans ce cas, il n'est pas nécessaire d'installer ISA Management sur un autre ordinateur puisque l'administration à distance peut s'effectuer à partir d'une session des services Terminal Server.

Conditions préalables à la mise en cache avancée

ISA Server peut être déployé en tant que serveur de mise en cache avancée gérant un cache centralisé d'objets Internet fréquemment demandés et accessible à l'aide de n'importe quel navigateur Web. Dans ce cas, évaluez le nombre de navigateurs Web qui doivent accéder à Internet. Le tableau ci-dessous répertorie les configurations matérielles en fonction du nombre estimé de clients internes accédant aux objets Internet.

Nombre d'utilisateurs	Configuration minimale de ISA Server	RAM (en Mo)	Espace disque alloué pour la mise en cache
Jusqu'à 500	Un seul ordinateur ISA Server avec processeur Pentium II 300 MHz	256	2 à 4 Gigaoctets (Go)
500–1,000	Un seul ordinateur ISA Server avec deux processeurs Pentium III 550 MHz	256	10 Go
Plus de 1 ;000	Deux ordinateurs ISA Server avec chacun deux processeurs Pentium III 550 MHz	256 par serveur	10 Go par serveur

Si votre base d'utilisateurs comprend plus de 1 ;000 utilisateurs, vous pouvez utiliser des ordinateurs avec des processeurs plus puissants et davantage de mémoire ou ajouter d'autres installations ISA Server. Pour plus d'informations, voir "Ajout d'ordinateurs".

Si vous configurez plus d'un ordinateur ISA Server, considérez une migration vers ISA Server Enterprise Edition de manière à pouvoir les rassembler en groupe. Pour plus d'informations, voir le chapitre 5, "Mise à niveau vers ISA Server, Enterprise Edition".

Configuration requise pour la publication (mise en cache inversée)

Le cache ISA Server peut être déployé afin de répondre aux demandes Web extérieures à l'entreprise. Vous pouvez, par exemple, placer un ISA Server entre Internet et le serveur Web d'une organisation qui héberge une activité commerciale sur le Web ou qui permet d'accéder à des partenaires commerciaux. Dans ce cas, considérez la fréquence à laquelle les clients externes demanderont des objets sur les serveurs de publication.

Le tableau ci-dessous dresse la liste des configurations matérielles requises pour des nombres attendus de requêtes provenant d'utilisateurs Internet (externes) dans un scénario de mise en cache inversée.

Accès par seconde **ISA Server**

Moins de 100	Un seul ISA Server avec processeur Pentium II 300 MHz
Jusqu'à 250	Un seul ISA Server avec processeur Pentium III 450 MHz
Plus de 250	Un ISA Server avec processeur Pentium III 550 MHz. Pour chaque ensemble de 250 accès supplémentaires par seconde, ajoutez un ISA Server supplémentaire. Vous pouvez également utiliser l'Analyseur de performances pour déterminer les goulets d'engorgement et ajouter des serveurs ou un matériel plus performant, si nécessaire.

La configuration mémoire requise dépend de la taille du contenu pouvant être mis en cache que vous publiez, l'idéal étant que ce contenu puisse être placé dans la mémoire disponible. Par exemple, si le site Web que vous publiez représente 256 Mo de contenu, 256 Mo de RAM suffisent.

Ajout d'ordinateurs

Vous pouvez utiliser les recommandations sur la planification de la capacité décrites ci-avant comme lignes directrices pour déterminer le nombre d'ordinateurs ISA Server dont vous avez besoin. Dans certains cas, vous devez choisir entre l'ajout d'un ISA Server supplémentaire ou l'amélioration des performances de l'ordinateur existant par ajout d'un autre processeur. Chaque option offre ses avantages.

Si vous ajoutez un ordinateur ISA Server, considérez une migration vers ISA Server Enterprise Edition de manière à pouvoir rassembler les serveurs ISA dans un groupe, et configurer un système à tolérance de pannes. En cas de défaillance d'un ordinateur, l'autre ordinateur continue à fonctionner. En outre, la gestion de groupe centralisée de ISA Server minimise les problèmes de gestion lors de l'ajout de serveurs supplémentaires au groupe.

En revanche, l'ajout d'un ordinateur vous contraint à acheter et gérer de nouveaux matériels ainsi que les logiciels installés sur l'ordinateur, tels que le système d'exploitation.

Sélection des fonctionnalités ISA Server

Vous pouvez installer ISA Server avec les fonctionnalités de pare-feu et de mise en cache, ou seulement l'une de ces deux fonctionnalités. Lors de la procédure d'installation, vous choisissez le mode d'installation : pare-feu, cache ou intégré.

En mode pare-feu, vous pouvez sécuriser les communications réseau en définissant des règles qui régissent les communications entre votre réseau d'entreprise et Internet. Vous pouvez également publier des serveurs internes et partager les données de vos serveurs internes avec des utilisateurs Internet.

En mode cache, vous pouvez améliorer les performances du réseau et économiser de la bande passante en stockant les objets souvent demandés plus près des utilisateurs. Vous pouvez ensuite acheminer les requêtes provenant d'utilisateurs Internet vers le serveur Web approprié.

En mode intégré, toutes les fonctionnalités de cache et de pare-feu sont disponibles. Vous pouvez établir une stratégie qui prend en compte les besoins en performances de cache et les besoins de sécurité.

Selon le mode sélectionné, vous disposez de différentes fonctionnalités. Le tableau ci-dessous répertorie les fonctionnalités disponibles pour les modes pare-feu et cache. En mode intégré, vous disposez de toutes les fonctionnalités.

Sélection des fonctionnalités ISA Server

Fonctionnalité	Pare-feu	Cache
Stratégie d'accès	Oui	Oui (protocoles HTTP et HTTPS uniquement)
Filtres d'application	Oui	Non
Configuration du cache	Non	Oui
Prise en charge des clients pare-feu et SecureNAT	Oui	Non

Filtrage de paquets	Oui	Non
Surveillance en temps réel	Oui	Oui
Rapports	Oui	Oui
Publication de serveur	Oui	Non
Réseau privé virtuel	Oui	Non
Filtres Web	Oui	Oui
Publication sur le Web	Oui	Oui
Prise en charge des clients proxy Web	Oui	Oui

Évaluation des besoins des clients

ISA Server prend en charge les types de clients suivants :

- I *Clients proxy Web.* Un client proxy Web envoie directement les requêtes à ISA Server, mais l'accès à Internet est limité au navigateur. Vous pouvez configurer les navigateurs Web prenant en charge HTTP (Hypertext Transfer Protocol) 1.1 comme clients proxy Web ;
- I *Clients SecureNAT.* Les clients SecureNAT assurent les fonctions de sécurité et de mise en cache mais ne permettent pas l'authentification au niveau de l'utilisateur. Pour configurer un client SecureNAT, il suffit d'attribuer l'adresse IP (Internet protocol) de ISA Server à la passerelle par défaut sur l'ordinateur client. Le client SecureNAT ne nécessitant pas d'autre configuration que le changement de la passerelle par défaut, tout ordinateur utilisant TCP/IP (Transmission Control Protocol/Internet Protocol) peut devenir un client SecureNAT ;
- I *Clients pare-feu.* Les clients pare-feu restreignent l'accès sur une base par utilisateur pour l'accès sortant des demandes qui utilisent les protocoles TCP et UDP (User Datagram Protocol). Pour configurer un client pare-feu, vous devez installer le logiciel client pare-feu sur chaque ordinateur client. Ce logiciel ne peut être installé que sur les ordinateurs exécutant Microsoft Windows Millennium Edition, Microsoft Windows 95 OSR2, Microsoft Windows 98, Windows NT 4.0 ou Windows 2000.

Avant de déployer ou de configurer le logiciel client, évaluez les besoins de votre entreprise. Déterminez les applications et les services dont vos clients internes ont besoin. Déterminez comment vous publierez les serveurs, puis établissez les correspondances entre ces besoins et les types de clients pris en charge par ISA Server.

Si vous souhaitez

Utilisez...

Améliorer les performances des requêtes Web pour les clients internes.

Les clients proxy Web.

Éviter de déployer le logiciel client ou de configurer les ordinateurs clients.

Les clients SecureNAT qui ne requièrent ni logiciel, ni configuration spécifique.

Améliorer les performances Web dans un environnement utilisant des systèmes d'exploitation autres que Microsoft.

Les clients SecureNAT. Les requêtes des clients sont transmises en toute transparence au service de pare-feu ISA Server, puis au service de mise en cache.

Publier les serveurs situés sur votre réseau interne.

Les clients SecureNAT. Les serveurs internes peuvent être publiés en tant que clients SecureNAT, ce qui vous évite de devoir créer des paramètres de configuration spéciaux sur le serveur de publication. Il est déconseillé de configurer

des serveurs de publication en tant que clients pare-feu.

Autoriser l'accès Internet aux utilisateurs authentifiés uniquement.

Les clients pare-feu. Vous pouvez configurer les règles de stratégie d'accès en fonction des utilisateurs pour les clients pare-feu.

Interaction avec d'autres services réseau

Vous avez peut-être utilisé le service Routage et accès distant de Windows 2000 pour permettre aux clients distants d'accéder aux ordinateurs et aux services du réseau. ISA Server fournit la connectivité à distance et étend les fonctions de routage et d'accès distant en proposant des fonctionnalités plus complètes et plus souples. Le filtrage de paquets de ISA Server remplace celui du service Routage et accès distant. ISA Server utilise les connexions d'accès à distance que vous avez configurées pour le service Routage et accès distant.

De la même manière, vous avez peut-être déjà utilisé les fonctionnalités Partage de connexion Internet (ICS) ou Traduction d'adresses réseau (NAT) de Windows 2000 pour accéder à Internet. ISA Server peut être utilisé à la place de NAT ou d'ICS, à la fois pour les remplacer et les améliorer au sein de l'entreprise. ISA Server fournit la même connectivité que NAT ou ICS et y ajoute des fonctionnalités performantes en matière de sécurité et de mise en cache.

Installation de ISA Server

Ce chapitre vous explique l'installation de Microsoft Internet Security and Acceleration (ISA) Server.

Il comprend les sections suivantes :

- I Avant d'installer ISA Server
- I Installation de ISA Server
- I Étapes suivantes

Avant d'installer ISA Server

Avant d'installer ISA Server, vous devez configurer le matériel et le logiciel de l'ordinateur qui va exécuter ISA Server.

Consultez les informations des sections suivantes pour vérifier que ISA Server répond aux caractéristiques de préinstallation requises. Pour plus d'informations sur une tâche, consultez la documentation fournie avec votre matériel ou avec Microsoft Windows 2000.

Configuration de la carte réseau

Vous pouvez connecter votre réseau à Internet par l'intermédiaire d'une connexion directe (T1, T3, xDSL ou modem câble) ou d'une connexion d'accès à distance. Si vous choisissez une connexion directe, vous devez configurer une carte réseau connectant ISA Server à Internet.

Lorsque vous définissez les propriétés TCP/IP (Transmission Control Protocol/Internet Protocol) pour la carte de réseau externe, adressez-vous à votre fournisseur de services Internet (ISP) pour savoir quels sont les paramètres requis. Vous avez notamment besoin de connaître l'adresse IP, le masque de sous-réseau, la passerelle par défaut et les adresses IP des serveurs DNS à utiliser dans les recherches de noms DNS. Dans certains cas, votre fournisseur de services Internet utilise le protocole DHCP (Dynamic Host Configuration Protocol) ou BOOTP (Bootstrap Protocol) pour l'attribution dynamique des adresses des clients.

En principe, ISA Server possède une seule passerelle IP (Internet Protocol) par défaut. Vous devez configurer l'adresse IP de la passerelle par défaut uniquement sur la réseau externe, pas sur la carte réseau interne. N'indiquez rien pour le paramètre de passerelle par défaut de la carte interne.

Reportez-vous à l'aide en ligne de Windows pour les instructions de configuration des cartes réseau.

Paramètres TCP/IP

Lorsque vous définissez les propriétés de TCP/IP d'une carte réseau interne, vous devez spécifier une adresse IP permanente réservée à ISA Server et un masque de sous-réseau pour votre réseau local. Les adresses attribuées par DHCP ne doivent pas être utilisées pour la carte réseau interne, car elles risquent de réinitialiser la passerelle par défaut que vous avez sélectionnée pour ISA Server. La carte réseau externe peut être activée pour DHCP ou son adresse IP peut être définie de façon statique, avec notamment la passerelle par défaut et les paramètres DNS.

Après la configuration, lancez l'utilitaire Ping.exe fourni avec Windows 2000 Server ou un utilitaire similaire sur un autre ordinateur client IP interne afin de vérifier la connectivité du réseau et vous assurer que les cartes réseau et les autres matériels sont correctement configurés.

Configuration d'un modem ou d'une carte RNIS

Si vous décidez de vous connecter à Internet via une connexion d'accès à distance au lieu d'une connexion directe au moyen d'une carte réseau externe, vous devez utiliser un modem ou une carte RNIS (Réseau numérique à intégration des services) avec votre serveur.

Selon la carte RNIS, il n'est pas toujours possible de visualiser les deux canaux RNIS dans Windows 2000. En général, les pilotes de la carte RNIS gèrent une connectivité basée sur la bande passante pour le deuxième canal ; vous ne pouvez pas utiliser Windows 2000 pour gérer le pilote. Vérifiez que la carte réseau permet la configuration des deux canaux et que votre fournisseur de services Internet prend en charge la connexion avec les deux canaux.

Pour plus d'informations sur la configuration d'une carte RNIS ou d'un modem, consultez l'aide de Windows 2000.

Table de routage Windows 2000

La table des adresses locales contient toutes les plages d'adresses IP internes utilisées par le réseau interne situé derrière ISA Server. ISA Server utilise la table des adresses locales afin de contrôler la façon dont les machines du réseau interne communiquent avec les réseaux externes et décide quelles cartes réseau doivent être protégées en chargeant le pilote de filtre de paquets.

ISA Server peut construire la table LAT en se basant sur la table de routage Windows 2000. Vous pouvez également sélectionner les plages d'adresses IP privées, telles qu'elles sont définies par l'instance IANA dans RFC 1918. Ces trois blocs d'adresses sont exclusivement réservés aux Intranet privés et ne sont jamais utilisés sur le réseau Internet public.

Si l'ordinateur est connecté à un réseau interne routé et que vous n'êtes pas certain de votre topologie de routage ou ne savez pas comment ajouter des routes statiques, vous pouvez créer manuellement la table afin qu'elle contienne la ou les plages des adresses IP utilisées par vos clients internes.

Une passerelle par défaut ne pouvant pas être définie sur l'interface interne de ISA Server, vous devrez créer par la suite des routes statiques pour votre réseau interne afin d'obtenir une connectivité totale. Pour ce faire, lancez la commande ROUTE de Windows 2000 à partir d'une invite de commande.

Une table des adresses locales correctement configurée permet à ISA Server de déterminer quel carte réseau utiliser afin d'accéder à différentes parties de votre réseau interne. Si la table de routage n'est pas définie correctement, la table des adresses locales ne peut pas être créée correctement. Il se peut donc qu'une demande client pour une adresse IP interne soit routée incorrectement vers Internet ou réacheminée via le service Firewall.

Si nécessaire, après l'installation, modifiez manuellement la table des adresses locales afin qu'elle comprenne tous les autres segments de réseau internes de votre organisation, notamment ceux de routeurs internes, afin que ISA Server et les clients pare-feu puissent correctement déterminer quand utiliser ISA Server et quand accéder directement à une ressource.

Lorsque vous créez une table LAT, n'indiquez que les adresses du réseau privé. Vous ne devez ajouter ni l'interface externe de ISA Server, ni des sites Internet, ni d'autres adresses externes comprenant le serveur DNS de votre fournisseur de services Internet, et autres. Une configuration incorrecte de la table des adresses locales risquerait de rendre votre réseau vulnérable aux attaques.

La table des adresses locales est gérée centralement car elle est administrée sur ISA Server. Les clients pare-feu téléchargent et reçoivent automatiquement les actualisations de la table des adresses locales à intervalles réguliers prédéfinis.

Installation de ISA Server

Lorsque vous installez ISA Server, il vous sera demandé les informations suivantes.

- I *Code CD-ROM.* Il s'agit du numéro à 10 chiffres situé au dos du boîtier du CD-ROM ISA Server.
- I *Options d'installation.* Vous avez le choix entre une installation standard, complète ou personnalisée.

- I *Mode*. Vous pouvez installer ISA Server en mode pare-feu, cache ou intégré.
- I *Configuration du cache*. Si vous installez ISA Server en mode intégré ou cache, vous devez configurer les lecteurs de cache que vous souhaitez utiliser ainsi que la taille du cache.
- I *Configuration de la Table d'adresses locales*. Si vous installez ISA Server en mode intégré ou pare-feu, vous devez configurer les plages d'adresses à inclure dans la Table d'adresses locales.

Important : vous devez installer Windows 2000 Service Pack 1 ou une version supérieure avant d'installer ISA Server.

Pour installer le logiciel serveur

1. Insérez le CD-ROM ISA Server dans le lecteur ou exécutez ISAautorun.exe à partir du dossier réseau partagé.
2. Dans le programme d'installation de Microsoft ISA Server, cliquez sur **Installer ISA Server**.
3. Si vous acceptez les termes et conditions du contrat de licence logicielle de l'utilisateur final, cliquez sur **Continuer**.
4. Entrez le numéro d'identification du produit situé sur la boîte.
5. Lisez le contrat de licence logicielle de l'utilisateur final et si vous en acceptez les termes et conditions, cliquez sur **J'accepte**.
6. Cliquez sur **Installation standard**, **Installation complète** ou **Installation personnalisée**.

Si vous cliquez sur **Installation personnalisée**, activez les cases à cocher qui correspondent aux composants ISA Server que vous souhaitez installer. Les choix suivants sont possibles :

- i Services ISA
 - i Services complémentaires
 - i Utilitaires d'administration
7. Cliquez sur le mode ISA Server à installer.
 8. Lorsque le programme d'installation vous avertit qu'il va arrêter IIS (Internet Information Service), si vous avez choisi d'installer ISA Server en mode cache ou intégré, configurez les lecteurs de cache.
 9. Si vous installez ISA Server en mode pare-feu ou intégré, configurez la table des adresses locales.
 10. Si vous souhaitez lancer l'Assistant Mise en route lorsque vous appelez ISA Server, cochez la case **Assistant Mise en route de l'administrateur ISA**.

Remarque

1. Le programme d'installation arrête le service IIS Web parce que son port par défaut est 80, le port http standard. ISA Server utilise ce port pour la publication Web et surveille les requêtes Web sur ces ports à partir de clients internes et externes lorsque les règles de publication Web sont définies.
2. Les lecteurs de disque disponibles pour la mise en cache peuvent être sélectionnés pendant l'installation d'ISA Server. Par défaut, l'installation recherche la plus grande partition NTFS et définit une taille de cache par défaut de 100 Mo si au moins 150 Mo sont disponibles. Lors de la configuration des lecteurs de cache, vous devez allouer au minimum un lecteur NTFS, en réservant au moins 5 Mo de cache sur ce lecteur. Toutefois, il est recommandé d'allouer au moins 100 Mo et d'ajouter 0,5 Mo pour chaque client utilisant les protocoles HTTP ou FTP, en arrondissant cette capacité au méga-octet supérieur.

Étapes suivantes

Après l'installation, ISA Server bloque toute communication entre le réseau de votre entreprise et Internet. Tant que vous ne configurez pas de stratégie d'accès, avec des règles de protocole, de site et de contenu autorisant précisément les accès, aucune communication ne sera autorisée. De même, vous devez configurer des règles de publication si vous souhaitez autoriser les clients Internet à accéder aux ordinateurs de votre réseau interne.

Paramètres par défaut après l'installation

Après l'installation, ISA Server utilise les paramètres par défaut suivants.

Fonctionnalité Paramètre par défaut

Autorisations utilisateur	Les membres du groupe Administrateurs sur l'ordinateur local peuvent configurer la stratégie.
Table d'adresses locales	Contient les entrées spécifiées pendant l'installation.
Filtrage de paquets	Activé en mode pare-feu et intégré Désactivé en mode cache.
Contrôle d'accès	Une règle par défaut de sites et de contenus appelée "Autoriser la règle" permet à tous les clients d'accéder en permanence à tous les contenus de tous les sites. Cependant, étant donné qu'aucune règle de protocole n'est définie, aucun trafic n'est autorisé.
Publication	Aucun serveur interne n'est accessible aux clients externes. Une règle par défaut de publication Web rejette toutes les demandes.
Routage	Toutes les demandes de clients proxy Web sont directement récupérées directement sur Internet.
Mise en cache	La taille du cache est définie selon la taille spécifiée durant l'installation. La mise en cache HPPT et FTP est activée. La mise en cache active est désactivée.
Alertes	Toutes les alertes sont actives, à l'exception des alertes suivantes : attaque par analyse de tous les ports, paquets ignorés, violation de protocole et attaque par bombe UDP.
Configuration des clients	Lors de l'installation ou de la configuration du client pare-feu et du client proxy Web, la détection automatique est activée. Les navigateurs Web des clients pare-feu sont configurés lors de l'installation d'un client pare-feu.

Assistant Mise en route

Une fois ISA Server installé, vous pouvez l'utiliser pour implémenter la sécurité de votre entreprise et les règles d'accès à Internet. La première étape consiste à créer les éléments de la stratégie décrivant votre réseau. Regroupez les ordinateurs en séries d'adresses client et les utilisateurs en groupes de sécurité de Windows 2000. Créez des ensembles de destinations incluant des ordinateurs et des domaines sur Internet. Définissez les protocoles pouvant être utilisés pour communiquer avec Internet. Utilisez ensuite les éléments de la stratégie lors de la création des règles de stratégie qui implémentent les règles de l'entreprise.

L'Assistant Mise en route vous guide pas à pas dans les étapes de définition et de configuration des stratégies initiales d'entreprise et de groupe. À la fin de cette procédure, vous avez configuré ISA Server pour sécuriser la connexion de votre réseau à Internet.

L'Assistant Mise en route vous aide à effectuer les tâches ci-dessous :

- I création d'éléments de stratégie que vous utiliserez lors de l'établissement des règles de stratégie ;
- I création de règles de protocoles et de règles de sites et de contenus ;
- I définition d'un niveau de sécurité du système et configuration du filtrage de paquets ;
- I configuration du routage et du chaînage afin de déterminer comment les demandes des clients sont routées vers le serveur de destination ;

- I création d'une stratégie de cache afin de déterminer quels objets sont mis en cache ;

Une fois la stratégie de ISA Server configurée, lisez le chapitre 5 pour savoir comment installer et configurer les clients de votre réseau. Lisez ensuite le chapitre 6 qui contient des exemples précis de scénarios de déploiement.

<< **1** 2 >>

Dernière mise à jour le mercredi 21 mars 2001

Pour en savoir plus

- I [Déploiement du pare-feu de sécurité, du serveur proxy et du cache Web chez Microsoft](#)
- I [Toutes les infos de TechNet sur le thème de la sécurité](#)
- I [Microsoft Internet Security and Acceleration Server 2000 Enterprise Edition - Guide d'installation et de déploiement](#)



Cette information provient de l'espace [Microsoft TechNet](#)
La source d'information indispensable pour les spécialistes de l'informatique en entreprise !