

Sophos Enterprise Manager

Guide de configuration des stratégies

Version du produit : 4.7

Date du document : juillet 2011



Table des matières

1	À propos de ce guide.....	3
2	Recommandations d'utilisation générale des stratégies.....	4
3	Paramétrage d'une stratégie de mise à jour.....	5
4	Paramétrage des stratégies antivirus et HIPS.....	6
5	Paramétrage des stratégies de pare-feu.....	9
6	Paramétrage des stratégies de contrôle des périphériques.....	15
7	Paramétrage des stratégies de protection antialtération.....	18
8	Recommandations de contrôle.....	20
9	Utilisation des contrôles sur accès.....	21
10	Utilisation des contrôles planifiés.....	22
11	Utilisation des contrôles à la demande	23
12	Exclusion d'éléments du contrôle.....	24
13	Support technique.....	25
14	Mentions légales.....	26

1 À propos de ce guide

Ce guide vous propose des instructions de configuration des stratégies pour Sophos Enterprise Manager.

En particulier, il vous aide à :

- Comprendre les conseils d'utilisation des stratégies.
- Configurer et déployer chaque stratégie par type.
- Utiliser les options de contrôle pour rechercher les éléments.
- Déterminer quels éléments à exclure du contrôle.

Ce guide s'adresse à vous si :

- Vous utilisez l'Enterprise Manager.
- Vous voulez des conseils sur les meilleures options à utiliser pour la configuration et le déploiement des stratégies.

Consultez le *Guide de démarrage de Sophos Enterprise Manager* avant de lire ce guide.

Tous les documents concernant l'Enterprise Manager sont disponibles sur http://www.sophos.fr/support/docs/Enterprise_Manager-all.html.

2 Recommandations d'utilisation générale des stratégies

Lorsque vous installez l'Enterprise Manager, les stratégies par défaut sont créées. Ces stratégies s'appliquent à tous les groupes que vous créez. Les stratégies par défaut sont conçues pour garantir un niveau efficace de protection. Si vous souhaitez utiliser des fonctions telles que le contrôle des périphériques ou de protection anti-altération, créez de nouvelles stratégies ou modifiez les stratégies par défaut.

Remarque : vous pouvez créer jusqu'à quatre nouvelles stratégies de chaque type.

Lors du paramétrage des stratégies, envisagez les actions suivantes :

- Utilisez les paramètres par défaut de la stratégie lorsque cela est possible.
- Prenez en compte le rôle de l'ordinateur lors du changement des paramètres de la stratégie par défaut ou lors de la création de nouvelles stratégies (par exemple, un ordinateur de bureau ou un serveur).
- Utilisez l'Enterprise Manager pour tous les paramètres de stratégie centralisés et définissez les options dans l'Enterprise Manager plutôt que sur l'ordinateur lui-même lorsque c'est possible.
- Définissez les options sur l'ordinateur lui-même uniquement lorsque vous avez besoin d'une configuration temporaire pour cet ordinateur ou pour les éléments pour lesquels la configuration centralisée est impossible comme les options de contrôle avancées.
- Créez un groupe et une stratégie séparés pour les ordinateurs nécessitant une configuration spéciale à longue échéance.

3 Paramétrage d'une stratégie de mise à jour

La stratégie de mise à jour spécifie les ordinateurs qui reçoivent les nouvelles définitions de menaces et les mises à jour des logiciels Sophos. Un abonnement logiciels permet de spécifier quelles versions des logiciels pour ordinateurs d'extrémité sont téléchargées depuis Sophos pour chaque plate-forme. La stratégie de mise à jour par défaut vous permet d'installer et de mettre à jour les logiciels spécifiés dans l'abonnement "Recommandé". Lors du paramétrage de votre stratégie de mise à jour, envisagez les actions suivantes :

- Par défaut, les ordinateurs se mettent à jour à partir d'un seul emplacement principal. Toutefois, nous vous conseillons de configurer également un emplacement secondaire de mise à jour. Si les ordinateurs d'extrémité ne sont pas en mesure de contacter leur source principale, ils tentent de se mettre à jour depuis leur source secondaire si elle a été spécifiée. Pour plus d'informations, reportez-vous à l'Aide de Sophos Enterprise Manager.
- Autorisez l'itinérance sur une stratégie de mise à jour pour les utilisateurs d'ordinateurs portables qui effectuent de nombreux déplacements professionnels au sein de votre entreprise. Lorsque l'option est activée, les ordinateurs portables itinérants recherchent et se mettent à jour à partir de l'emplacement des serveurs de mise à jour le plus proche en envoyant des requêtes aux ordinateurs d'extrémité fixes se trouvant sur le même réseau local auxquels ils sont connectés, réduisant ainsi les délais de mise à jour et les coûts de bande passante. S'il reçoit plusieurs emplacements, l'ordinateur portable détermine lequel est le plus proche et l'utilise. Si aucun emplacement ne fonctionne, l'ordinateur portable utilise l'emplacement principal (puis l'emplacement secondaire) défini dans sa stratégie de mise à jour. L'itinérance fonctionne uniquement si l'ordinateur d'extrémité itinérant se met à jour à partir d'un emplacement administré par la même instance de l'Enterprise Manager qui gère l'ordinateur d'extrémité. Pour plus d'informations, reportez-vous à l'Aide de Sophos Enterprise Manager.
- Assurez-vous que le nombre de groupes utilisant la même stratégie de mise à jour est gérable. Vous ne devez généralement pas avoir plus de 1000 ordinateurs procédant à la mise à jour à partir du même emplacement. Le nombre idéal pour une mise à jour optimale depuis le même emplacement est de 600-700 ordinateurs.

Remarque : le nombre d'ordinateurs pouvant se mettre à jour depuis le même répertoire dépend du serveur contenant ce répertoire et de la connectivité du réseau. Toutefois, sachez que vous pouvez créer au maximum quatre nouvelles stratégies de mise à jour dans l'Enterprise Manager.

- Si vous êtes préoccupé par les problèmes de performances sur des ordinateurs dont les spécifications sont plus basses, vous pouvez exécuter les mises à jour moins souvent (deux ou trois fois par jour) ou à des heures précises en dehors des heures de travail habituelles des utilisateurs (en soirée ou le week-end).



Avertissement : la réduction des mises à jour augmente les risques de menaces pour votre sécurité.

4 Paramétrage des stratégies antivirus et HIPS

4.1 Paramètres recommandés

La stratégie antivirus et HIPS définit la manière dont le logiciel de sécurité effectue le contrôle des ordinateurs à la recherche de virus, chevaux de Troie, vers, spywares, adwares, applications potentiellement indésirables (PUA), comportements et fichiers suspects et la manière dont il les nettoie. Lorsque vous paramétrez votre stratégie antivirus et HIPS, envisagez les actions suivantes :

- La stratégie antivirus et HIPS par défaut assure la protection des ordinateurs contre les virus et autres malwares. Toutefois, vous pouvez créer de nouvelles stratégies ou changer la stratégie par défaut pour activer la détection d'autres applications ou comportements indésirables.
- Utilisez la protection Live Sophos qui, grâce à son service de recherche en ligne, décide instantanément si un fichier suspect est une menace et qui effectue la mise à jour en temps réel de votre logiciel Sophos. L'option **Activer la protection Live** est activée par défaut. Pour profiter pleinement de la protection Live Sophos, nous vous conseillons également de sélectionner l'option **Envoyer automatiquement les échantillons de fichiers à Sophos**.
- Utilisez l'option **Alerter uniquement** pour détecter uniquement les comportements suspects. Si vous définissez d'abord une stratégie qui édite uniquement des rapports, ceci vous permettra d'avoir une meilleure visibilité des comportements suspects sur votre réseau. Cette option est activée par défaut et doit être désélectionnée dès que le déploiement de la stratégie est terminé afin de bloquer les programmes et les fichiers.

4.2 Comment déployer la stratégie antivirus et HIPS ?

Nous vous conseillons de déployer la stratégie antivirus et HIPS comme suit :

1. Créez des stratégies différentes pour des groupes différents. Toutefois, sachez que vous pouvez créer au maximum quatre nouvelles stratégies antivirus et HIPS dans l'Enterprise Manager.
2. Déterminez les exclusions du contrôle sur accès pour les répertoires ou les ordinateurs avec des bases de données volumineuses ou des fichiers qui changent fréquemment. Assurez-vous par ailleurs que les contrôles planifiés sont exécutés. Vous pouvez, par exemple, exclure des répertoires particuliers sur les serveurs Exchange ou sur d'autres serveurs sur lesquels les performances peuvent être affectées. Pour plus d'informations, consultez l'article 12421 de la base de connaissances du support de Sophos (<http://www.sophos.fr/support/knowledgebase/article/12421.html>).
3. Définissez les options de la protection Live Sophos. Cette fonction offre la protection la plus récente contre les menaces grâce à son service de recherche en ligne qui décide

instantanément si un fichier suspect est une menace et grâce à la mise à jour en temps réel de votre logiciel Sophos. Les options suivantes sont disponibles :

- **Activer la protection Live** : si le contrôle antivirus identifie un fichier comme étant suspect sur l'ordinateur mais ne peut pas déterminer s'il s'agit d'un fichier sain ou malveillant en se basant sur les fichiers d'identité des menaces (IDE) présents sur l'ordinateur, certaines caractéristiques du fichier (sa somme de contrôle et d'autres attributs) sont envoyés à Sophos pour une analyse approfondie. Le service de recherche en ligne de Sophos effectue une recherche instantanée d'un fichier suspect dans la base de données des SophosLabs. Si le fichier est identifié comme sain ou malveillant, la décision est renvoyée à l'ordinateur et l'état du fichier est automatiquement mis à jour.

Cette option est activée par défaut.

- **Envoyer automatiquement les échantillons de fichiers à Sophos** : si un fichier est jugé potentiellement malveillant mais ne peut pas être identifié avec certitude comme malveillant d'après ses seules caractéristiques, la protection Live Sophos permet à Sophos de demander un échantillon du fichier. Si l'option **Envoyer automatiquement les échantillons de fichiers à Sophos** est activée et si Sophos ne détient encore pas d'échantillon du fichier, ce dernier sera soumis automatiquement. L'envoi de tels échantillons de fichiers aide Sophos à améliorer en permanence la détection des malwares sans aucun risque de faux positifs.

Important : assurez-vous que le domaine Sophos auquel les données des fichiers sont envoyées est fiable dans votre solution de filtrage Web. Pour plus de détails, consultez l'article 62637 de la base de connaissances du support technique de Sophos (<http://www.sophos.fr/support/knowledgebase/article/62637.html>). Si vous utilisez une solution Sophos de filtrage Web, par exemple l'appliance Web WS1000, aucune opération de votre part n'est nécessaire. Les domaines sont déjà fiables.

4. Détectez les virus et les spywares.
 - a) Assurez-vous que le contrôle sur accès est activé ou planifiez un contrôle intégral du système pour détecter les virus et les spywares. Le contrôle sur accès est activé par défaut. Pour plus d'informations, reportez-vous aux sections [Utilisation des contrôles sur accès](#) à la page 21 ou [Utilisation des contrôles planifiés](#) à la page 22.
 - b) Sélectionnez les options de nettoyage pour les virus/spywares.
5. Détectez les fichiers suspects.

Les fichiers suspects contiennent certaines caractéristiques communes à celles des programmes malveillants mais pas suffisamment pour que le fichier soit identifié comme une nouvelle pièce de malware.

 - a) Activez le contrôle sur accès ou planifiez un contrôle intégral du système pour détecter les fichiers suspects.
 - b) Sélectionnez l'option **Fichiers suspects (HIPS)**.
 - c) Sélectionnez les options de nettoyage des fichiers suspects.
 - d) Autorisez, si nécessaire, tous les fichiers dont l'exécution est permise.
6. Détectez les comportements suspects et les dépassements de la mémoire tampon.

Les détections des comportements suspects et des dépassements de la mémoire tampon surveillent continuellement les processus en cours pour déterminer si un programme affiche un comportement suspect. Ces détections sont utiles pour colmater les failles de sécurité.

- a) Utilisez l'option **Alerter uniquement** pour ne détecter que les comportements suspects et les dépassements de la mémoire tampon. Cette option est activée par défaut.
- b) Autorisez tous les programmes ou fichiers que vous souhaitez continuer à exécuter à l'avenir.
- c) Configurez votre stratégie pour bloquer les programmes et fichiers qui sont détectés en dessélectionnant l'option **Alerter uniquement**.

Cette approche évite le blocage des programmes et des fichiers dont vos utilisateurs pourraient avoir besoin. Pour plus d'informations, consultez l'article 50160 de la base de connaissances du support de Sophos (<http://www.sophos.fr/support/knowledgebase/article/50160.html>).

7. Déterminez les adwares et les PUA.

Lorsque vous lancez un contrôle à la recherche d'adwares et de PUA pour la première fois, le contrôle peut générer un grand nombre d'alertes pour les applications qui sont déjà en cours d'exécution sur votre réseau. En commençant par exécuter un contrôle planifié, vous traitez de manière plus sûre les applications qui sont déjà en cours d'exécution sur votre réseau.

- a) Planifiez un contrôle intégral du système pour détecter tous les adwares et PUA.
- b) Autorisez ou désinstallez toutes les applications détectées par le contrôle.
- c) Sélectionnez l'option de contrôle sur accès **Adwares et PUA** pour détecter les adwares et les PUA à venir.

Pour plus d'informations, consultez l'article 13815 de la base de connaissances du support de Sophos (<http://www.sophos.fr/support/knowledgebase/article/13815.html>).

8. Déterminez les menaces dans les pages Web.

- a) Assurez-vous que l'option **Bloquer l'accès aux sites Web malveillants** est définie sur **Activé** pour garantir le blocage des sites Web malveillants. Cette option est activée par défaut.
- b) Paramétrez l'option **Contrôle des téléchargements** sur **Activé** ou sur **Identique à celui sur accès** pour contrôler et bloquer toutes données malveillantes téléchargées. L'option **Identique à celui sur accès**, paramètre par défaut, active le contrôle des téléchargements seulement lorsque le contrôle sur accès est activé.
- c) Selon le cas, autorisez tous les sites Web qui sont autorisés.

Pour plus d'informations sur le paramétrage de la stratégie antivirus et HIPS, reportez-vous à l'Aide du Sophos Enterprise Manager

5 Paramétrage des stratégies de pare-feu

5.1 À propos de la stratégie de pare-feu

La stratégie de pare-feu définit la manière dont le pare-feu assure la protection des ordinateurs. Seules les applications nommées ou les classes d'applications sont autorisées à accéder au réseau de l'entreprise ou à Internet.

Remarque : Sophos Client Firewall n'est pas pris en charge sur les systèmes d'exploitation serveur. Pour voir les configurations requises en matière de matériels et de systèmes d'exploitation, consultez la page Configuration requise sur le site Web de Sophos (<http://www.sophos.fr/products/all-sysreqs.html>).



Avertissement : configurez la stratégie de pare-feu avant utilisation. Le déploiement d'une stratégie par défaut non modifiée dans un groupe via l'Enterprise Manager entraînera des problèmes avec les communications réseau.

La stratégie de pare-feu par défaut n'est pas prévue pour un déploiement "telle quelle" et n'est pas adaptée à une utilisation normale. Il s'agit d'une base pour vous aider à créer votre propre stratégie.

Par défaut, le pare-feu est activé et bloque tout le trafic réseau non indispensable. Tout ce qui n'a pas trait au réseau de base, par exemple, votre logiciel de messagerie, votre navigateur Web et tout accès réseau à la base de données, ne fonctionnera probablement pas correctement avec la stratégie par défaut qui bloque toutes les connexions non essentielles. Par conséquent, configurez-le pour qu'il autorise le trafic, les applications et les processus que vous souhaitez utiliser et testez-le avant d'installer et d'exécuter le pare-feu sur tous les ordinateurs.

5.2 Planification des stratégies de pare-feu

Planifiez vos stratégies de pare-feu ainsi que ce que vous souhaitez qu'elles fassent avant de créer ou de modifier les règles de pare-feu (globale, application ou autre).

Lorsque vous planifiez vos stratégies de pare-feu, vous devez prendre en compte :

- Quels ordinateurs doivent avoir Sophos Client Firewall.
- Si un ordinateur est un poste de bureau ou un portable. Il peut être judicieux de paramétrer un emplacement double pour les ordinateurs portables.
- Quelle méthode de détection de l'emplacement vous voulez utiliser, la recherche DNS ou la détection des adresses MAC à la passerelle.
- Les systèmes et protocoles réseau.
- Les connexions distantes.

D'après les applications et les droits d'accès réseau requis par les différents groupes d'utilisateurs, décidez combien de stratégies de pare-feu vous devez créer. Vous pouvez créer au maximum quatre nouvelles stratégies de pare-feu. Les stratégies couvrent différentes applications et

varient en termes de restrictions. Sachez que plusieurs stratégies requièrent plusieurs groupes dans l'Enterprise Manager.

- N'utilisez pas une seule stratégie Sophos Client Firewall. Vous seriez forcé d'ajouter des règles pour seulement un ou deux ordinateurs (par exemple, la station de travail de l'administrateur) et ces règles seraient présentes sur l'ensemble du réseau. C'est un risque pour la sécurité.
- Inversement, l'utilisation de différentes configurations signifie du temps supplémentaire passé à la surveillance et la maintenance.

Systèmes et protocoles réseau

Prenez en compte les services sur lesquels compte votre réseau. Par exemple :

- DHCP
- DNS
- RIP
- NTP
- GRE

Des règles existent dans la configuration du pare-feu par défaut pour couvrir la plupart de ces services. Par contre, sachez lesquels vous devez autoriser et ceux dont vous n'avez pas besoin.

Accès distant aux ordinateurs

Si vous utilisez un logiciel d'accès à distance pour surveiller et réparer les ordinateurs, créez dans votre configuration des règles qui vous permettront de fonctionner ainsi.

Identifiez les technologies que vous utiliser pour accéder aux ordinateurs sur votre réseau. Par exemple :

- RDP
- Client/serveur VPN
- SSH/SCP
- Terminal services
- Citrix

Vérifiez quelle sorte d'accès est nécessaire et créez vos règles en conséquence.

5.3 Paramètres recommandés

Lors du paramétrage de votre stratégie de pare-feu, envisagez les actions suivantes :

- Quand Sophos Client Firewall est installé, le pare-feu Windows est désactivé. Par conséquent, si vous utilisez le pare-feu Windows, notez les configurations existantes et déplacez-les dans le Sophos Client Firewall.
- Utilisez le mode **Autoriser par défaut** pour détecter le trafic, les applications et les processus, mais sans les bloquer. En définissant d'abord une stratégie qui édite uniquement des rapports, vous aurez une meilleure visibilité de l'activité du réseau.

- Utilisez l'Observateur d'événements du pare-feu pour voir le trafic, les applications et les processus utilisés. L'Observateur d'événements vous facilite également la tâche de création de règles d'autorisation ou de blocage du trafic, des applications et des processus signalés. Vous accédez à l'Observateur d'événements en cliquant sur **Affichage > Événements du pare-feu**.
- Examinez les règles créées via l'Observateur d'événements. Une application peut déclencher plusieurs événements de pare-feu, mais une règle d'application doit couvrir toutes les actions d'application.
- Autorisez l'utilisation d'un navigateur Web, de la messagerie électronique et du partage de fichiers et d'imprimantes.
- Nous vous recommandons de ne pas changer les paramètres ICMP par défaut, les règles globales et les règles d'applications sauf si vous êtes un utilisateur confirmé en administration réseau.
- Nous vous recommandons dans la mesure du possible de créer des règles d'applications plutôt que des règles globales.
- N'utilisez pas le mode **Interactif** dans une stratégie où un emplacement double est configuré.
- N'utilisez pas le mode **Interactif** sur des réseaux de grande ou de moyenne taille et dans des environnements de domaine. Le mode **Interactif** peut être utilisé pour créer des règles de pare-feu sur de très petits réseaux (par exemple, jusqu'à 10 ordinateurs) dans des environnements de groupe de travail et sur des ordinateurs autonomes.

5.4 Configuration du pare-feu en emplacement double

L'option d'emplacement unique s'adresse aux ordinateurs qui sont connectés en permanence à un réseau unique comme les postes de travail. L'option d'emplacement double est disponible si vous voulez que le pare-feu utilise des paramètres différents en fonction de l'emplacement où les ordinateurs sont utilisés, par exemple, au bureau et en dehors du bureau. Il peut être judicieux de paramétrer un emplacement double pour les ordinateurs portables.

Si vous sélectionnez l'emplacement double, nous vous recommandons de paramétrer vos options de configuration d'emplacement principal et secondaire comme suit :

- Paramétrez votre emplacement principal en tant que réseau que vous contrôlez (par exemple, le réseau professionnel) et votre emplacement secondaire en tant qu'emplacement étant hors de votre contrôle.
- Paramétrez votre emplacement principal de manière à ce qu'il ait un accès plus facile et votre emplacement secondaire de manière à ce qu'il ait un accès plus restreint.
- Lors de la configuration de vos options de détection de l'emplacement principal, nous recommandons généralement d'utiliser la détection DNS sur des réseaux étendus et complexes et d'utiliser la détection passerelle pour les réseaux de petite taille et simples. La détection DNS nécessite l'utilisation d'un serveur DNS mais elle est généralement plus facile à gérer que la détection passerelle. Si le matériel utilisé pour la détection passerelle tombe en panne, la reconfiguration des adresses MAC est nécessaire et il est possible que les ordinateurs reçoivent par erreur la configuration de l'emplacement secondaire tant que les problèmes de configuration matérielle ne sont pas résolus.

- Si vous utilisez la détection DNS, nous vous recommandons d'ajouter une entrée DNS spécifique à votre serveur DNS dont le nom est inhabituel et qui renvoie une adresse IP localhost également appelée adresse de bouclage ou loopback (127.x.x.x). Ces options rendent pratiquement impossible la détection incorrecte de tout autre réseau auquel vous êtes connecté comme étant votre emplacement principal.
- Dans la section "Emplacement appliqué" de la configuration avancée de la stratégie de pare-feu, sélectionnez la configuration du pare-feu que vous souhaitez appliquer à l'ordinateur. Si vous souhaitez que la configuration appliquée dépende de l'emplacement de l'ordinateur, sélectionnez l'option **Appliquer la configuration pour l'emplacement détecté**. Si vous souhaitez appliquer manuellement la configuration principale ou secondaire, sélectionnez l'option appropriée.



Avertissement : il est vivement recommandé d'utiliser avec précaution les règles de sous-réseau local comme configurations secondaires. S'il s'agit d'un ordinateur portable utilisé en dehors du bureau, il peut se connecter à un sous-réseau inconnu. Dans ce cas, il se peut que les règles de pare-feu de la configuration secondaire qui utilisent l'adresse du sous-réseau local autorisent le trafic inconnu.

5.5 Comment déployer une stratégie de pare-feu ?

Déployez une stratégie qui vous permette de surveiller tout le trafic passant par votre réseau. Vous recevrez des rapports de trafic dans l'Observateur d'événements du pare-feu. Utilisez ces informations pour paramétrer une stratégie de base.

Exécutez un déploiement par phases du Sophos Client Firewall sur votre réseau. Déployez, par exemple, Sophos Client Firewall dans un groupe à la fois. Ainsi, vous évitez d'inonder votre réseau de trafic au cours des premières étapes.



Avertissement : tant que la configuration n'a pas été soigneusement vérifiée et testée, ne procédez pas au déploiement sur l'ensemble de votre réseau .

1. Déployez Sophos Client Firewall sur un groupe test d'ordinateurs, représentatif des divers rôles sur votre réseau.
2. Configurez une stratégie de pare-feu pour utiliser le mode **Autoriser par défaut** afin de détecter (mais sans bloquer) le trafic, les applications et les processus habituels, et attribuez la stratégie au groupe test.
 - a) Créez une nouvelle stratégie de pare-feu. Dans le volet **Stratégies** de l'Enterprise Manager, cliquez avec le bouton droit de la souris sur **Pare-feu** et sélectionnez **Créer une stratégie**. Donnez un nom à cette stratégie, puis cliquez deux fois dessus.
Autrement, modifiez la stratégie par défaut : Dans le volet **Stratégies**, cliquez deux fois sur **Pare-feu** puis cliquez deux fois sur **Par défaut**.

L'assistant de **Stratégie de pare-feu** apparaît.

- b) Choisissez d'utiliser l'assistant en cliquant sur **Suivant** ou de configurer la stratégie manuellement en cliquant sur **Stratégie de pare-feu avancée**.
 - À l'aide de l'assistant : cliquez sur **Suivant**. Sélectionnez **Emplacement unique** et cliquez sur **Suivant**. Sélectionnez **Surveiller**, cliquez sur **Suivant**, puis de nouveau sur **Suivant**, puis sur **Terminer**.
 - À l'aide de l'option **Stratégie de pare-feu avancée** : dans la boîte de dialogue **Stratégie de pare-feu**, près de **Emplacement principal**, cliquez sur **Configurer**. Dans l'onglet **Général**, définissez le mode de fonctionnement sur **Autoriser par défaut**. Cliquez sur **OK**, puis de nouveau sur **OK**.
 - c) Attribuez la nouvelle stratégie de pare-feu au groupe test.
3. Utilisez l'Observateur d'événements du pare-feu pour voir le trafic, les applications et les processus utilisés. L'Observateur d'événements vous facilite également la tâche de création de règles d'autorisation ou de blocage du trafic, des applications et des processus signalés. Vous accédez à l'Observateur d'événements en cliquant sur **Affichage > Événements du pare-feu**.
 4. Surveillez les événements du pare-feu et créez votre stratégie sur une certaine période, par exemple, sur deux semaines.
 - a) Créez des règles dans l'Observateur d'événements. Cliquez avec le bouton droit de la souris sur un événement pour lui créer une règle. Pour plus d'informations sur la création de règles de pare-feu, reportez-vous à la section "Configuration de stratégies" > "Configuration de la stratégie de pare-feu" de l'Aide du Sophos Enterprise Manager.
 - b) Recherchez toutes les faiblesses de la stratégie (par exemple, un accès trop large attribué à certains utilisateurs).
 - c) En cas de besoins différents, procédez à une sous-division du groupe et créez des stratégies et des règles supplémentaires si nécessaire.
 5. Examinez les règles créées via l'Observateur d'événements. Une application peut déclencher plusieurs événements de pare-feu, mais une règle d'application doit couvrir toutes les actions d'application.
 6. Divisez le reste de votre réseau en groupes facilement administrables et représentatifs des multiples rôles sur un réseau, par exemple, stations de travail des commerciaux, stations de travail des administrateurs informatiques, etc.. Toutefois, sachez que vous pouvez créer au maximum quatre nouvelles stratégies de pare-feu dans l'Enterprise Manager.
 7. Une fois que vous pensez tout couvrir, par exemple, lorsque vous n'obtenez plus de nouveaux événements de pare-feu pour lesquels il n'y a pas de règles, créez des stratégies à partir de vos règles et attribuez-les selon les besoins. Si vous avez un nombre important d'ordinateurs sur votre réseau, nous vous conseillons de déployer Sophos Client Firewall sur un groupe à la fois.
 8. Dès que vous avez testé les règles, changez le mode de stratégie sur **Bloquer par défaut**, sinon les ordinateurs demeureront non sécurisés.

Pour plus d'informations sur le paramétrage d'une stratégie de pare-feu, reportez-vous à la section "Configuration des stratégies" > "Configuration de la stratégie de pare-feu" de l'Aide de Sophos Enterprise Manager.

Remarque : comme alternative à la surveillance du trafic réseau et à la création de règles à l'aide de l'Observateur d'événements de pare-feu, sur un très petit réseau ou sur des ordinateurs autonomes, vous pouvez installer Sophos Client Firewall sur un ordinateur de test et le configurer en mode **Interactif**. Lancez autant d'applications que possible sur votre réseau, y compris des navigateurs Web. Puis importez et modifiez la configuration du pare-feu contenant des règles établies par ce processus. Pour plus d'informations, consultez l'Aide de Sophos Endpoint Security and Control.

6 Paramétrage des stratégies de contrôle des périphériques

6.1 Paramètres recommandés

La stratégie de contrôle des périphériques spécifie quels périphériques de stockage et de réseau sont autorisés à être utilisés sur les ordinateurs. Lors du paramétrage de la stratégie de contrôle des périphériques, envisagez les actions suivantes :

- Utilisez l'option **Détecter mais ne pas bloquer les périphériques** pour détecter les périphériques contrôlés sans les bloquer. Vous devez tout d'abord paramétrer l'état sur **Bloqué** pour chaque type de périphérique que vous voulez détecter. Le logiciel ne contrôle pas les types de périphériques que vous n'avez pas spécifiés. Si vous définissez d'abord une stratégie qui édite uniquement des rapports, ceci vous permettra d'avoir une meilleure visibilité des périphériques utilisés sur tout votre réseau.
- Utilisez l'Observateur d'événements du contrôle des périphériques pour filtrer plus rapidement les événements bloqués que vous souhaitez consulter. Vous accédez à l'Observateur d'événements en cliquant sur **Affichage > Événements du contrôle des périphériques**.
- Utilisez le Gestionnaire des rapports pour créer des rapports de tendance sur les événements de contrôle des périphériques par ordinateur ou par utilisateur.
- Envisagez un contrôle d'accès plus sévère pour les utilisateurs ayant un accès aux informations sensibles.
- Préparez une liste d'exemptions de périphériques avant de déployer une stratégie qui va bloquer les périphériques. Par exemple, si vous souhaitez autoriser l'utilisation des lecteurs optiques à votre équipe de création artistique.
- La catégorie "Périphériques de stockage amovibles sécurisés" peut être utilisée pour autoriser automatiquement les périphériques de stockage USB chiffrés de différents fabricants que nous prenons en charge. Une liste complète de ces fabricants est disponible sur le site Web de Sophos. Pour une liste des périphériques de stockage amovibles sécurisés pris en charge, consultez l'article 63102 de la base de connaissances du support de Sophos (<http://www.sophos.fr/support/knowledgebase/article/63102.html>).
- Utilisez le champ **Commentaire** pour identifier la raison de l'exemption d'un périphérique ou pour savoir qui a demandé cette exemption lors de l'ajout d'exemptions de périphériques à la stratégie de contrôle des périphériques.
- Utilisez les options de messagerie de bureau personnalisées pour offrir plus d'assistance à vos utilisateurs lors de la découverte d'un périphérique contrôlé. Par exemple, vous pouvez fournir un lien vers la stratégie d'utilisation des périphériques de votre entreprise.
- Si vous souhaitez activer un périphérique réseau (par exemple, un adaptateur wifi) lorsque l'ordinateur est physiquement déconnecté du réseau, sélectionnez l'option **Bloquer le pont** lors du paramétrage des niveaux d'accès pour les périphériques réseau.

Remarque : le mode Bloquer le pont réduit de manière significative les risques de pont de réseau entre un réseau professionnel et un réseau non professionnel. Ce mode est disponible

pour les types de périphériques sans fil et modem. Ce mode fonctionne en désactivant les adaptateurs réseau sans fil ou modem lorsqu'un ordinateur d'extrémité est connecté à un réseau physique (généralement, via une connexion Ethernet). Une fois l'ordinateur déconnecté du réseau physique, les adaptateurs réseau sans fil ou modem sont réactivés de manière transparente.

- Soyez sûr de vouloir bloquer un périphérique avant de déployer votre stratégie. Assurez-vous de bien connaître tous les cas de figure d'utilisation, surtout ceux liés à la WiFi et aux périphériques réseau.



Avertissement : toute modification des stratégies s'effectue à partir du serveur de l'Enterprise Manager vers l'ordinateur via le réseau, par conséquent, dès que le réseau est bloqué, il ne peut pas être débloqué depuis l'Enterprise Manager étant donné que l'ordinateur n'accepte aucune configuration supplémentaire à partir du serveur.

6.2 Comment déployer une stratégie de contrôle des périphériques ?

Par défaut, le contrôle des périphériques est désactivé et tous les périphériques sont autorisés. Nous vous recommandons d'introduire le contrôle des périphériques comme suit :

1. Déterminez les périphériques que vous voulez contrôler.
2. Activez le contrôle des périphériques et sélectionnez l'option **Détecter mais ne pas bloquer les périphériques** pour détecter les périphériques contrôlés, mais sans les bloquer. Vous devez tout d'abord paramétrer l'état sur **Bloqué** pour chaque type de périphérique que vous voulez détecter. Le logiciel ne contrôle pas les types de périphériques que vous n'avez pas spécifiés.
Vous avez, à présent, une stratégie de contrôle des périphériques pour tout votre réseau.
3. Utilisez l'Observateur d'événements du contrôle des périphériques pour voir quelles périphériques sont en cours d'utilisation et pour déterminer les types de périphériques que vous souhaitez bloquer. Vous accédez à l'Observateur d'événements en cliquant sur **Affichage > Événements du contrôle des périphériques**.
4. Pour accorder un accès différent aux périphériques selon les multiples groupes d'ordinateurs, créez des stratégies différentes pour des groupes différents. Par exemple, vous pouvez ne pas vouloir autoriser l'accès des périphériques de stockage amovibles à vos services des ressources humaines et de finances, mais accepter de l'autoriser à votre service informatique et de ventes. Toutefois, sachez que vous pouvez créer au maximum quatre nouvelles stratégies de contrôle des périphériques dans l'Enterprise Manager.
5. Exemptez les instances ou les types de modèle que vous ne souhaitez pas bloquer. Par exemple, vous pouvez exempter une clé USB spécifique (instance) ou tous les modems Vodafone 3G (type de modèle).
6. Déterminez quels périphériques vous voulez bloquer et changez leurs états sur **Bloqués**. Vous pouvez aussi autoriser l'accès en lecture seule à certains périphériques de stockage.
7. Configurez votre stratégie pour bloquer les périphériques contrôlés qui sont détectés en dessélectionnant l'option **Détecter mais ne pas bloquer les périphériques**.

En choisissant cette approche, vous évitez de générer un grand nombre d'alertes et de bloquer les périphériques dont vos utilisateurs pourraient avoir besoin. Pour plus d'informations sur

le paramétrage d'une stratégie de contrôle des périphériques, reportez-vous à l'Aide du Sophos Enterprise Manager.

7 Paramétrage des stratégies de protection antialtération

7.1 Paramètres recommandés

La protection antialtération vous permet d'empêcher les utilisateurs (administrateurs locaux aux connaissances techniques limitées) de reconfigurer, de désactiver ou de désinstaller les logiciels de sécurité Sophos. Les utilisateurs qui ne connaissent pas le mot de passe de la protection antialtération ne peuvent pas exécuter ces opérations.

Remarque : la protection antialtération n'est pas conçue pour assurer une protection contre les utilisateurs expérimentés techniquement. Elle n'assure pas la protection contre les programmes malveillants spécifiquement conçus pour corrompre le fonctionnement du système d'exploitation afin d'éviter d'être détecté. Ce type de malware sera uniquement détecté en effectuant un contrôle à la recherche de menaces et de comportements suspects. Pour plus d'informations, reportez-vous à la section [Paramétrage des stratégies antivirus et HIPS](#) à la page 6.

Après avoir activé la protection antialtération et créé un mot de passe pour celle-ci, l'utilisateur qui ne connaît pas ce mot de passe ne pourra pas reconfigurer les détections du contrôle sur accès ou des comportements suspects dans Sophos Endpoint Security and Control, désactiver la protection antialtération ou désinstaller les composants Sophos Endpoint Security and Control (Sophos Anti-Virus, Sophos Client Firewall, Sophos AutoUpdate ou Sophos Remote Management System) ou Sophos SafeGuard Disk Encryption du Panneau de configuration.

Lors du paramétrage de votre stratégie de protection antialtération, envisagez les actions suivantes :

- Utilisez l'Observateur d'événements de la protection antialtération pour vérifier l'utilisation du mot de passe de la protection antialtération et surveiller la fréquence des tentatives d'altération dans votre entreprise. Vous pouvez visualiser à la fois les événements d'authentification réussis de la protection antialtération (utilisateurs autorisés passant outre la protection antialtération) et les échecs de tentative d'altération des logiciels de sécurité Sophos. Vous accédez à l'Observateur d'événements en cliquant sur **Affichage > Événements de protection antialtération**.

7.2 Comment déployer une stratégie de protection antialtération ?

Par défaut, la protection antialtération est désactivée. Nous vous conseillons d'introduire la stratégie de protection antialtération comme suit :

1. Activez la protection antialtération et créez un mot de passe fort pour la protection antialtération.

Le mot de passe permet uniquement aux utilisateurs d'ordinateurs d'extrémité autorisés de reconfigurer, désactiver ou désinstaller le logiciel de sécurité Sophos.

Remarque : la protection antialtération n'affecte pas les membres des groupes SophosUser et SophosPowerUser. Lorsque la protection antialtération est activée, ces utilisateurs peuvent tout de même réaliser toutes les tâches qu'ils ont généralement l'autorisation d'exécuter, sans qu'il soit nécessaire de saisir le mot de passe de la protection antialtération.

2. Si vous avez besoin d'activer ou de désactiver la protection antialtération ou de créer des mots de passe différents pour divers groupes, créez des stratégies différentes pour les différents groupes. Toutefois, sachez que vous pouvez créer au maximum quatre nouvelles stratégies de protection antialtération dans l'Enterprise Manager.

Pour plus d'informations sur le paramétrage d'une stratégie de protection antialtération, reportez-vous à l'Aide du Sophos Enterprise Manager.

8 Recommandations de contrôle

Les options de contrôle dans les sections suivantes sont définies dans la stratégie antivirus et HIPS. Lors du choix des options de contrôle, envisagez les actions suivantes :

- Utilisez les paramètres par défaut à chaque fois que c'est possible.
- Définissez le contrôle dans l'Enterprise Manager ainsi que sur l'ordinateur lui-même, si possible.
- Prenez en compte le rôle de l'ordinateur (par exemple, ordinateur de bureau ou serveur).

Extensions

Pour accéder aux options d'extension pour le contrôle sur accès, dans la boîte de dialogue **Stratégie antivirus et HIPS**, cliquez sur **Configurer** près de **Activer le contrôle sur accès**, puis allez sur l'onglet **Extensions**.

Pour les contrôles planifiés, dans la boîte de dialogue **Stratégie antivirus et HIPS**, sous **Contrôle planifié**, cliquez sur **Extensions et exclusions**.

- L'option **Contrôler tous les fichiers** n'est généralement pas nécessaire ou pas recommandée. Sélectionnez plutôt l'option **Contrôler uniquement les exécutables et autres fichiers vulnérables** pour rechercher les menaces découvertes par les SophosLabs. Procédez au contrôle de tous les fichiers uniquement après avoir pris conseil auprès du support technique.

Autres options de contrôle

Pour accéder aux autres options de contrôle sur accès, dans la boîte de dialogue **Stratégie antivirus et HIPS**, cliquez sur **Configurer** près de **Activer le contrôle sur accès**.

Pour les contrôles planifiés, dans la boîte de dialogue **Stratégie antivirus et HIPS**, sous **Contrôle planifié**, sélectionnez un contrôle et cliquez sur **Modifier**. Dans la boîte de dialogue **Paramètres du contrôle planifié**, cliquez sur **Configurer**.

- L'option **Contrôler dans les fichiers archive** ralentit le contrôle et n'est généralement pas requise. Lorsque vous tentez d'accéder au contenu d'un fichier archive, ce fichier est contrôlé automatiquement. Par conséquent, nous vous recommandons de ne pas sélectionner cette option sauf si vous utilisez fréquemment des fichiers archive.
- Nous vous recommandons d'effectuer le contrôle de la mémoire système d'un ordinateur à la recherche des menaces. La mémoire système est utilisée par le système d'exploitation. Vous pouvez contrôler la mémoire système de manière périodique en tâche de fond alors que le contrôle sur accès est activé. Vous pouvez aussi inclure le contrôle de la mémoire système dans le cadre d'un contrôle planifié. L'option **Contrôle de la mémoire système** est activée par défaut.

9 Utilisation des contrôles sur accès

Lorsque vous utilisez les contrôles sur accès, envisagez les actions suivantes :

- Utilisez les paramètres par défaut à chaque fois que cela est possible.
- Utilisez l'option de contrôle sur accès **En lecture**. Les options de contrôle **En écriture** et **En renommant** ne sont généralement pas requises mais sont mises à disposition si vous souhaitez bénéficier d'une sécurité maximale. Ces options sont utiles en cas d'épidémies virales.
- Le contrôle sur accès ne détecte pas les virus lorsque certains logiciels de chiffrement sont installés. Modifiez les processus de démarrage afin de vous assurer que ces fichiers sont déchiffrés lorsque le contrôle sur accès commence. Pour plus d'informations sur l'utilisation de la stratégie antivirus et HIPS avec un logiciel de chiffrement, consultez l'article 12790 de la base de connaissances du support de Sophos (<http://www.sophos.fr/support/knowledgebase/article/12790.html>).
- Lorsque vous ne sélectionnez pas le contrôle sur accès, assurez-vous que les ordinateurs utilisent les contrôles planifiés. Pour plus d'informations, reportez-vous à la section [Utilisation des contrôles planifiés](#) à la page 22.



Avertissement : la désactivation du contrôle sur accès augmente les risques de menaces pour votre sécurité.

10 Utilisation des contrôles planifiés

Lorsque vous utilisez les contrôles planifiés, envisagez les actions suivantes :

- Utilisez les paramètres par défaut à chaque fois que cela est possible.
- Utilisez les contrôles planifiés pour évaluer les menaces ou estimer la prédominance des applications non désirées ou contrôlées.
- Utilisez les contrôles planifiés sur les répertoires serveur sur lesquels les performances seront affectées par l'utilisation du contrôle sur accès. Par exemple, vous pouvez avoir un groupe de serveurs Exchange qui utilise les contrôles planifiés sur des répertoires spécifiques. Pour plus d'informations, consultez l'article 12421 de la base de connaissances du support de Sophos (<http://www.sophos.fr/support/knowledgebase/article/12421.html>).
- Lorsque vous ne sélectionnez pas le contrôle sur accès, assurez-vous que les ordinateurs utilisent les contrôles planifiés. Placez ces ordinateurs dans un groupe et définissez un contrôle planifié.
- Les contrôles planifiés peuvent affecter les performances. Par exemple, si vous procédez au contrôle d'un serveur qui lit les bases de données et y écrit dedans en permanence, prenez en compte le moment où ses performances seront le moins affectées.
- Pour les serveurs, prenez en compte les tâches en cours d'exécution. S'il y a une tâche de sauvegarde, n'exécutez pas le contrôle planifié en même temps que la tâche de sauvegarde.
- Procédez au contrôle à des heures définies. Assurez-vous qu'un contrôle planifié est effectué quotidiennement sur chaque ordinateur (par exemple, tous les jours à 21 heures). Les contrôles planifiés doivent être effectués au moins une fois par semaine sur les ordinateurs.
- L'option **Exécuter le contrôle avec une priorité inférieure** permet l'exécution d'un contrôle planifié sous les systèmes d'exploitation Windows Vista et supérieure avec une priorité inférieure afin que l'opération ait des conséquences minimales sur les applications de l'utilisateur. Cette option est conseillée, même si le contrôle prendra plus de temps que sans cette option.

11 Utilisation des contrôles à la demande

Lorsque vous utilisez les contrôles à la demande, envisagez les actions suivantes :

- Utilisez les contrôles à la demande lorsque l'évaluation ou le nettoyage manuel est nécessaire.

12 Exclusion d'éléments du contrôle

Procédez à l'exclusion d'éléments du contrôle de la manière suivante :

- Utilisez les extensions pour exclure des types de fichiers spécifiques du contrôle.
- Utilisez les exclusions pour exclure du contrôle des éléments spécifiques, tels que les fichiers ou les lecteurs. Vous pouvez créer des exclusions de lecteur (X:), des exclusions de répertoire (X:\Program Files\Exchsrvr\) ou des exclusions de fichier (X:\Program Files\SomeApp\SomeApp.exe).
- Envisagez d'exclure les périphériques multimédia du contrôle sur accès pour les utilisateurs spécifiques qui les utilisent énormément. Les lecteurs multimédia lisent et écrivent sur les fichiers temporaires et chaque fichier est intercepté et contrôlé à chacune de ses utilisations. Ceci a pour effet de ralentir le contrôle.
- Utilisez l'option **Exclure les fichiers distants** lorsque vous ne souhaitez pas contrôler des fichiers distants (sur les ressources du réseau). Nous vous conseillons de contrôler tous les fichiers distants sur accès, toutefois, vous pouvez sélectionner cette option sur les serveurs de fichiers ou lorsque des fichiers volumineux ou constamment modifiés font l'objet d'un accès à distance.



Avertissement : l'exclusion d'éléments du contrôle augmente les risques de menace pour votre sécurité.

13 Support technique

Le support technique pour les produits Sophos est disponible de l'une des manières suivantes :

- Rendez-vous sur le forum de la communauté SophosTalk en anglais sur <http://community.sophos.com/> et recherchez d'autres utilisateurs rencontrant le même problème que le vôtre.
- Rendez-vous sur la base de connaissances du support de Sophos sur <http://www.sophos.fr/support/>.
- Téléchargez la documentation des produits sur <http://www.sophos.fr/support/docs/>.
- Envoyez un courriel à support@sophos.fr, y compris le ou les numéros de version du logiciel Sophos, le ou les systèmes d'exploitation et le ou les niveaux de correctif ainsi que le texte du ou des messages d'erreur.

14 Mentions légales

Copyright © 2011 Sophos Limited. Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, stockée dans un système de recherche documentaire ou transmise, sous quelque forme ou par quelque moyen que ce soit, électronique, mécanique, photocopie, enregistrement ou autre sauf si vous possédez une licence valide, auquel cas vous pouvez reproduire la licence conformément à ses termes ou si vous avez le consentement préalable écrit du propriétaire du copyright.

Sophos et Sophos Anti-Virus sont des marques déposées de Sophos Limited. Tous les autres noms de produits et de sociétés mentionnés sont des marques ou des marques déposées appartenant à leurs propriétaires respectifs.

ACE™, TAO™, CIAO™, and CoSMIC™

ACE¹, TAO², CIAO³, and CoSMIC⁴ (henceforth referred to as “DOC software”) are copyrighted by Douglas C. Schmidt⁵ and his research group⁶ at Washington University⁷, University of California⁸, Irvine, and Vanderbilt University⁹, Copyright © 1993–2005, all rights reserved.

Since DOC software is open-source, free software, you are free to use, modify, copy, and distribute—perpetually and irrevocably—the DOC software source code and object code produced from the source, as well as copy and distribute modified versions of this software. You must, however, include this copyright statement along with code built using DOC software.

You can use DOC software in commercial and/or binary software releases and are under no obligation to redistribute any of your source code that is built using DOC software. Note, however, that you may not do anything to the DOC software code, such as copyrighting it yourself or claiming authorship of the DOC software code, that will prevent DOC software from being distributed freely using an open-source development model. You needn't inform anyone that you're using DOC software in your software, though we encourage you to let us¹⁰ know so we can promote your project in the DOC software success stories¹¹.

DOC software is provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Moreover, DOC software is provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use, correction, modification, or enhancement. A number of companies¹² around the world provide commercial support for DOC software, however. DOC software is Y2K-compliant, as long as the underlying OS platform is Y2K-compliant.

Washington University, UC Irvine, Vanderbilt University, their employees, and students shall have no liability with respect to the infringement of copyrights, trade secrets or any patents by DOC software or any part thereof. Moreover, in no event will Washington University, UC Irvine, or Vanderbilt University, their employees, or students be liable for any lost revenue or profits or other special, indirect and consequential damages.

The ACE¹³, TAO¹⁴, CIAO¹⁵, and CoSMIC¹⁶ web sites are maintained by the DOC Group¹⁷ at the Institute for Software Integrated Systems (ISIS)¹⁸ and the Center for Distributed Object Computing of Washington University, St. Louis¹⁹ for the development of open-source software as part of the open-source software community²⁰. By submitting comments, suggestions, code, code snippets, techniques (including that of usage), and algorithms, submitters acknowledge

that they have the right to do so, that any such submissions are given freely and unreservedly, and that they waive any claims to copyright or ownership. In addition, submitters acknowledge that any such submission might become part of the copyright maintained on the overall body of code, which comprises the DOC software. By making a submission, submitter agree to these terms. Furthermore, submitters acknowledge that the incorporation or modification of such submissions is entirely at the discretion of the moderators of the open-source DOC software projects or their designees.

The names ACE, TAO, CIAO, CoSMIC, Washington University, UC Irvine, and Vanderbilt University, may not be used to endorse or promote products or services derived from this source without express written permission from Washington University, UC Irvine, or Vanderbilt University. Further, products or services derived from this source may not be called ACE, TAO, CIAO, or CoSMIC nor may the name Washington University, UC Irvine, or Vanderbilt University appear in their names, without express written permission from Washington University, UC Irvine, and Vanderbilt University.

If you have any suggestions, additions, comments, or questions, please let me²¹ know.

Douglas C. Schmidt²²

References

1. <http://www.cs.wustl.edu/~schmidt/ACE.html>
2. <http://www.cs.wustl.edu/~schmidt/TAO.html>
3. <http://www.dre.vanderbilt.edu/CIAO/>
4. <http://www.dre.vanderbilt.edu/cosmic/>
5. <http://www.dre.vanderbilt.edu/~schmidt/>
6. <http://www.cs.wustl.edu/~schmidt/ACE-members.html>
7. <http://www.wustl.edu/>
8. <http://www.uci.edu/>
9. <http://www.vanderbilt.edu/>
10. mailto:doc_group@cs.wustl.edu
11. <http://www.cs.wustl.edu/~schmidt/ACE-users.html>
12. <http://www.cs.wustl.edu/~schmidt/commercial-support.html>
13. <http://www.cs.wustl.edu/~schmidt/ACE.html>
14. <http://www.cs.wustl.edu/~schmidt/TAO.html>
15. <http://www.dre.vanderbilt.edu/CIAO/>
16. <http://www.dre.vanderbilt.edu/cosmic/>
17. <http://www.dre.vanderbilt.edu/>
18. <http://www.isis.vanderbilt.edu/>
19. <http://www.cs.wustl.edu/~schmidt/doc-center.html>
20. <http://www.opensource.org/>
21. <mailto:d.schmidt@vanderbilt.edu>
22. <http://www.dre.vanderbilt.edu/~schmidt/>

Apache

Les logiciels Sophos mentionnés dans le présent document peuvent inclure des programmes logiciels concédés en licence (ou en sous licence) à l'utilisateur selon les termes de la licence

Apache. Une copie du contrat de licence pour chacun des logiciels inclus est disponible sur <http://www.apache.org/licenses/LICENSE-2.0>.

Common Public License

Les logiciels Sophos auxquels le présent document fait référence incluent ou peuvent inclure des programmes logiciels concédés en licence (ou en sous licence) à l'utilisateur selon les termes de la licence Common Public License (CPL), qui, entre autres droits, permettent à l'utilisateur d'avoir accès au code source. La licence CPL exige que pour tout logiciel concédé en licence sous les termes de la licence CPL, qui est distribuée sous un format de code objet, le code source soit aussi mis à disposition de ces utilisateurs sous un format de code objet. Pour chacun de ces logiciels couverts par la licence CPL, le code source est disponible sur commande par courrier postal envoyé à Sophos, par courrier électronique envoyé à support@sophos.fr ou par Internet sur <http://www.sophos.fr/support/queries/enterprise.html>. Une copie du contrat de licence pour chacun des logiciels inclus est disponible sur <http://opensource.org/licenses/cpl1.0.php>

ConvertUTF

Copyright 2001–2004 Unicode, Inc.

This source code is provided as is by Unicode, Inc. No claims are made as to fitness for any particular purpose. No warranties of any kind are expressed or implied. The recipient agrees to determine applicability of information provided. If this file has been purchased on magnetic or optical media from Unicode, Inc., the sole remedy for any claim will be exchange of defective media within 90 days of receipt.

Unicode, Inc. hereby grants the right to freely use the information supplied in this file in the creation of products supporting the Unicode Standard, and to make copies of this file in any form for internal or external distribution as long as this notice remains attached.

iMatix SFL

This product uses parts of the iMatix SFL, Copyright © 1991-2000 iMatix Corporation
<http://www.imatix.com>.

OpenSSL cryptographic toolkit

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL license

Copyright © 1998–2006 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)”

4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (ey@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay license

Copyright © 1995–1998 Eric Young (ey@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (ey@cryptsoft.com). The implementation was written so as to conform with Netscape’s SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

“This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”

The word “cryptographic” can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

“This product includes software written by Tim Hudson (tjh@cryptsoft.com)”

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]