Livre blanc

Intégration des serveurs aux structures de sécurité modernes

L'univers où se trouvent vos serveurs a changé. Aujourd'hui, ces éléments clés de l'entreprise, riches en données, ne trouvent pas leur place dans votre structure de sécurité moderne. À vrai dire, cette dernière protège tout, sauf vos serveurs stratégiques. Pourtant, les obligations réglementaires exigent une protection des données identique pour tous.

Ce livre blanc fournit une méthode simple pour intégrer vos serveurs aux structures de sécurité modernes et enfin combler l'écart technologique, sans compromettre les opérations métiers.

opentext™

Sommaire

page

Le serveur, un élément isolé

Autrefois, les serveurs résidaient dans un univers sécurisé. Ils échangeaient des données en toute sécurité avec les terminaux. Le serveur connaissait l'utilisateur, la provenance des données et leur destination finale.

Mais les temps ont changé. Aujourd'hui, les réseaux sont ouverts, les architectures sont orientées services et la cybercriminalité fait rage. La sécurité des serveurs n'a pas suivi le rythme. La sécurité traditionnelle qui encadre l'accès aux serveurs laisse les données dangereusement exposées de bien des manières :

Authentification décentralisée et faible

Un simple mot de passe à huit caractères est peut-être le seul obstacle qui vient s'interposer entre un pirate informatique et vos données hôtes stratégiques. L'authentification basée sur le serveur ne peut pas à elle seule exploiter toute la puissance du système de gestion des identités utilisé par le reste de l'entreprise.

Autorisation décentralisée et faible

Dès lors qu'il est connecté au réseau de l'entreprise, un utilisateur accède facilement aux applications hôtes. Autrement dit, un pirate informatique a seulement besoin de voler les références à huit chiffres d'un utilisateur pour atteindre illégalement des champs de données personnelles.

Audit décentralisé

L'audit de l'accès aux serveurs est réalisé par chaque serveur en fonction de l'ID hôte de chaque utilisateur. Lorsque plusieurs serveurs sont impliqués, les administrateurs de la sécurité doivent examiner les journaux un par un, en comparant l'ID utilisateur de chaque serveur à l'ID utilisateur de l'entreprise, afin de concevoir un suivi d'audit complet.

Chiffrement problématique

Avant l'arrivée du chiffrement SSL/TLS dans les années 1990, les données et les mots de passe voyageaient entre le client et le serveur en texte clair. Il n'existait aucun moyen de mettre ces éléments à l'abri des regards indiscrets. Les protocoles SSL/TLS ont résolu le problème du chiffrement, mais avec un certain inconvénient : il est impossible de surveiller le trafic chiffré dans la zone démilitarisée, ce qui signifie que le service de sécurité IT est obligé d'autoriser le passage du trafic alors qu'il ignore tout de son contenu.

Manque de contrôle centralisé

Comme l'authentification, l'autorisation et l'audit ne peuvent être appliqués qu'individuellement à chaque serveur, il est difficile pour l'équipe centrale en charge de la sécurité de surveiller et garantir le respect des stratégies de sécurité de l'entreprise.

Étant donné la valeur de vos données hôtes stratégiques, il s'agit de failles de sécurité importantes. La question est de savoir comment protéger les données sans modifier les applications hôtes qui ont nécessité plusieurs décennies de développement. Comment pouvez-vous faire basculer vos serveurs dans le nouvel univers de la sécurité ?

Il faut dorénavant savoir se protéger des nouvelles menaces de sécurité qui émanent de fraudeurs aux méthodes toujours plus sophistiquées.

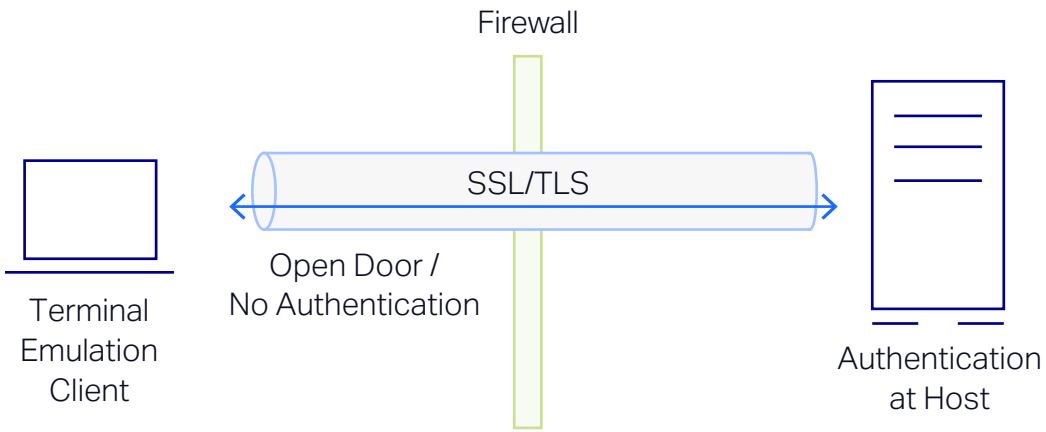

Figure 1. La sécurité des serveurs de première génération propose un chiffrement SSL/TLS de type « direct vers le serveur », mais l'authentification n'intervient qu'une fois que la connexion a atteint le serveur.

Les structures de sécurité modernes

Il faut dorénavant savoir se protéger des nouvelles menaces de sécurité qui émanent de fraudeurs aux méthodes toujours plus sophistiquées. Malheureusement, dans le domaine de la cybersécurité, aucune méthode n'est infaillible. La meilleure défense consiste à multiplier les couches de sécurité, ce qui inclut des technologies avancées d'authentification et d'autorisation, pour limiter les risques.

Par exemple, les agences informatiques gouvernementales américaines ont établi des infrastructures de clés publiques (PKI) et utilisent des cartes à puce pour prendre en charge les normes d'identification personnelle telles que PIV (FIPS 201). Ces types de contrôle sont adoptés petit à petit par les entités commerciales qui s'efforcent de respecter les nouvelles normes telles que PCI DSS, SOX et HIPAA.

Les systèmes de gestion des identités et des accès modernes n'ont jamais été conçus pour fonctionner avec des serveurs anciens, et inversement. Mais qu'en serait-il s'il était possible d'intégrer les deux systèmes, en étendant une sécurité robuste et centralisée aux applications hôtes, sans compromettre les opérations métiers ? Heureusement, il existe bien une solution : OpenText™ Host Access Management and Security Server (MSS).

L'ajout de couches de sécurité est une excellente approche qui peut être mise en oeuvre en plusieurs étapes. Ceci étant dit, une sécurité renforcée va de pair avec une gestion efficace. Voilà pourquoi les organisations mettent en oeuvre des systèmes de gestion des accès et des identités (IAM). Ces systèmes, tels qu'Active Directory, sont au coeur des structures de sécurité modernes. Ils permettent d'accorder, de révoquer et d'auditer l'accès aux données, aux ressources et aux applications de l'entreprise depuis un emplacement central unique.

Un problème demeure malgré tout : les systèmes IAM ne fonctionnent pas avec les serveurs Unisys, UNIX, HP et IBM de longue date qui contiennent énormément de données. De plus, l'intégration des deux systèmes n'est pas simple à réaliser. Il est difficile, risqué et onéreux de reconcevoir la logique de serveur qui régit votre entreprise, même si vous parvenez à mettre la main sur un programmeur de mainframe encore en activité. Il est également inacceptable d'affaiblir les références IAM complexes pour les adapter à des références de connexion hôte faibles. Les coûts associés sont tout simplement trop élevés.

En conséquence, vous disposez de deux infrastructures de sécurité distinctes : d'un côté, les serveurs, probablement gérés par RACF ou Top Secret. De l'autre côté, tout le reste, géré par le système IAM. Et ces deux infrastructures doivent respecter des exigences réglementaires toujours plus strictes.

Construire une alliance entre le serveur et l'IAM

Les systèmes de gestion des identités et des accès modernes n'ont jamais été conçus pour fonctionner avec des serveurs anciens, et inversement. Mais qu'en serait-il s'il était possible d'intégrer les deux systèmes, en étendant une sécurité robuste et centralisée aux applications hôtes, sans compromettre les opérations métiers ?

Heureusement, il existe bien une solution : OpenText™ Host Access Management and Security Server (MSS). MSS et ses extensions fonctionnent avec votre système IAM pour gérer et sécuriser de manière centralisée l'accès aux serveurs via vos émulateurs de terminal OpenText™ Reflection, OpenText™ Extra!, OpenText™ InfoConnect et OpenText™ Rumba+. Il s'agit d'une solution non intrusive qui ne nécessite aucune modification de vos applications hôtes ou de votre système IAM.

Pour chacune des catégories de sécurité qui suivent, nous allons expliquer le mode de fonctionnement des structures de sécurité modernes et comment les intégrer à vos serveurs à l'aide de MSS :

Authentification centralisée

Fonctionnement des structures de sécurité modernes : un système IAM applique des stratégies de sécurité et d'authentification rigoureuses à l'ensemble de l'entreprise.

Rôle de MSS : MSS inclut un serveur d'administration qui utilise le système IAM pour valider les références d'un utilisateur avant de lui accorder l'accès au serveur. En d'autres termes, les utilisateurs ne peuvent accéder à l'écran de connexion au serveur qu'après avoir été authentifiés et autorisés par le biais de références IAM complexes qui confirment leur identité. Vous pouvez dorénavant exiger la même authentification renforcée pour accéder aux serveurs que pour les autres systèmes.

MSS simplifie le processus d'intégration en prenant en charge tous les systèmes IAM courants, dont Active Directory, NetIQ eDirectory by OpenText™, IBM Tivoli Directory Server, OpenLDAP et Oracle Directory Server Enterprise Edition. Il prend également en charge toute une gamme de technologies d'authentification, dont Kerberos, NTLM, CRL, OCSP, PKI et les certificats X.509 utilisés avec des cartes à puce telles que CAC et PIV.

Autorisation centralisée

Fonctionnement des structures de sécurité modernes : un système IAM garantit que les utilisateurs n'accèdent qu'aux ressources et informations nécessaires à leur travail et à rien d'autre.

Rôle de MSS : MSS permet d'étendre les schémas d'autorisation IAM à l'accès aux serveurs sans modifier ces derniers ni le workflow utilisateur. Par exemple, vous pouvez accorder ou refuser l'accès en fonction du groupe ou du rôle, ce qui permet, par exemple, à un utilisateur d'accéder au mainframe 3270 mais pas au serveur Unisys. Vous pouvez monter la sécurité d'un cran grâce au proxy de sécurité MSS. Ce proxy fournit un jeton signé numériquement, limité dans le temps, qui utilise la cryptographie à clé publique pour empêcher les utilisateurs non autorisés de se connecter au serveur.

Grâce à MSS, vous pouvez également préciser quelles tâches chaque utilisateur est habilité ou non à effectuer. Par exemple, vous pouvez durcir l'émulation de terminal, en supprimant la capacité d'un utilisateur à modifier les macros ou en verrouillant les paramètres de connexion pour TLS 1.2.

Le serveur d'administration MSS permet aussi d'effectuer des réglages à la volée après une installation. La prochaine fois que les utilisateurs démarreront une session, ils recevront les modifications.

MSS simplifie le processus d'intégration en prenant en charge tous les systèmes IAM courants, dont :

- Active Directory
- NetIQ eDirectory
- IBM Tivoli Directory Server ;
- OpenLDAP ;
- Oracle Directory Server Enterprise Edition.

Il prend également en charge une large gamme de technologies d'authentification, dont :

- Kerberos ;
- NTLM ;
- CRL ;
- OCSP ;
- PKI ;
- les certificats X.509 utilisés avec les cartes à puce telles que CAC et PIV.

Composants de MSS

La licence MSS comprend un serveur d'administration et un serveur de comptage. Les extensions suivantes apportent des fonctionnalités stratégiques supplémentaires :

Extension Security Proxy de MSS : appliquez un contrôle d'accès au périmètre au moyen d'une technologie de sécurité brevetée.

Extension Terminal ID Management de MSS : allouez dynamiquement des ID de terminal en fonction du nom d'utilisateur, du nom DNS, de l'adresse IP ou de la réserve d'adresses.

Extension Automated Sign-On for Mainframe de MSS : permettez aux utilisateurs de saisir leurs références une seule fois pour obtenir un accès autorisé à tous les systèmes de l'entreprise, mainframe compris.

Extension PKI Automated Sign-On de MSS : fournissez une connexion automatisée avec PKI à vos systèmes d'entreprise stratégiques.

Avec MSS et ses extensions, vous pouvez moderniser la sécurité des serveurs sans modifier les applications hôtes ni le système IAM.

Audit centralisé

Fonctionnement des structures de sécurité modernes : un système IAM consigne l'identité des utilisateurs, les ressources réseau auxquelles ils accèdent et la date et l'heure d'accès, ce qui fournit aux administrateurs réseau les données dont ils ont besoin pour respecter les exigences d'audit.

Rôle de MSS : MSS use le système IAM existant pour authentifier les utilisateurs et autoriser l'accès aux serveurs tout en consignant toutes les activités dans un emplacement centralisé. Ainsi, vous savez qui a accédé à quel serveur et à quel moment. Ce processus garantit également que vous pouvez présenter une preuve écrite lors des audits.

Chiffrement

Fonctionnement des structures de sécurité modernes : les données sont chiffrées au début de la transmission (à l'intérieur ou à l'extérieur du pare-feu) et déchiffrées à la réception. Même si ce processus protège les données, il empêche aussi leur inspection dans la zone démilitarisée.

Rôle de MSS : MSS fonctionne avec le proxy de sécurité MSS, qui se situe entre les postes de travail et les serveurs. Le proxy de sécurité accepte les paquets chiffrés via SSL/TLS et les déchiffre avant leur transmission au serveur. Une fois déchiffrés, les paquets peuvent être surveillés par des outils de détection d'intrus, d'inspection du contenu et d'autres périphériques de sécurité afin de prévenir les attaques ou les fuites de données potentielles.

Le proxy de sécurité MSS ne fonctionne pas comme une simple passerelle SSL/TLS ou un redirecteur qui accepterait les connexions SSL/TLS sans commencer par autoriser l'utilisateur. Ces types de solution offrent aux intrus une autoroute jusqu'au serveur. Avec MSS, les intrus qui tentent d'établir une connexion SSL/TLS au serveur (sans obtenir l'authentification et l'autorisation du serveur d'administration MSS) ne peuvent pas accéder au proxy de sécurité MSS. Le proxy de sécurité utilise un jeton sécurisé et breveté par Micro Focus (faisant désormais partie d'OpenText), ce qui garantit que seuls les utilisateurs autorisés accèdent aux ressources hôtes.

MSS prend en charge des puissances de chiffrement AES qui peuvent atteindre 256 bits. Il prend également en charge les modules cryptographiques validés pour FIPS 140-2, l'une des normes de sécurité les plus exigeantes de l'administration américaine. Ce niveau de sécurité élevé signifie que vous pouvez protéger votre serveur contre tout contenu malveillant. Il fournit aussi une structure qui permet d'ajouter des couches de sécurité si nécessaire.

Accès à plusieurs serveurs via un seul port

Fonctionnement des structures de sécurité modernes : il est possible d'accéder à plusieurs serveurs backend via un seul port d'écoute.

Rôle de MSS : MSS vous permet d'utiliser une seule ouverture dans le pare-feu (le port 443, par exemple) pour accéder à tous les serveurs. Vous pouvez ajouter d'autres serveurs par la suite, sans rien changer au pare-feu. Cette configuration simplifiée réduit non seulement le nombre de ports à surveiller, mais aussi la surface d'attaque du réseau.

Contrôle centralisé de la configuration

Fonctionnement des structures de sécurité modernes : le système IAM permet au service IT de sécuriser, gérer et déployer de manière centralisée une large gamme de configurations d'applications pour l'ensemble de l'entreprise.

Rôle de MSS : MSS vous permet de gérer les opérations d'accès aux serveurs depuis la console MSS centrale. Vous pouvez accorder ou refuser l'accès selon le groupe ou le rôle, appliquer rapidement des mises à jour de sécurité et des modifications de configuration afin de suivre l'évolution des besoins métiers et des exigences réglementaires, et effectuer des réglages à la volée après l'installation. Bref, vous pouvez configurer et verrouiller des centaines, voire des milliers de postes de travail très facilement. Et vous pouvez le faire selon votre emploi du temps et non celui de quelqu'un d'autre.

L'un des principaux avantages de MSS est qu'il tire parti des investissements existants dans le domaine de la sécurité pour autoriser, authentifier et auditer l'accès de l'émulation de terminal aux serveurs depuis un emplacement central. Par conséquent, les problèmes pratiques et logistiques liés à l'application de mesures de sécurité renforcées à chaque serveur backend sont considérablement réduits.

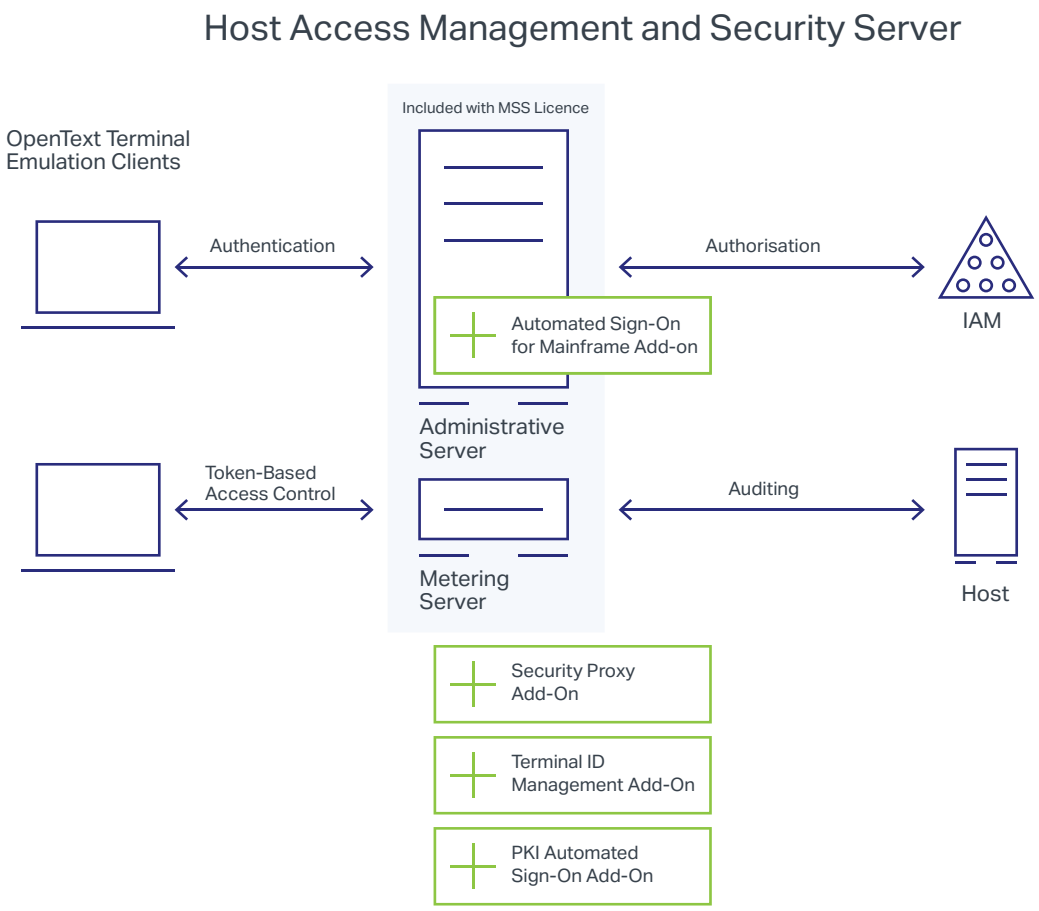

Figure 2. MSS fonctionne comme un point de contrôle d'accès en amont du serveur, ce qui oblige les utilisateurs à s'authentifier et à être autorisés avant d'accéder aux ressources hôtes.

Une protection identique pour tous

Grâce à MSS, vous pouvez enfin proposer une sécurité moderne à couches multiples pour assurer la protection de vos précieuses ressources hôtes sans modifier le serveur ni le système de gestion des identités et des accès. En intégrant ces deux systèmes d'entreprise stratégiques via MSS, vous pouvez :

- renforcer la sécurité des données et des applications hôtes stratégiques ;
- rationaliser la gestion des accès aux serveurs ;
- optimiser votre investissement IAM en étendant le système IAM aux serveurs ;
- faciliter le respect des exigences de sécurité les plus strictes ;
- moderniser la sécurité des serveurs sans perturber les workflows utilisateur ni les opérations métiers.

Testez MSS par vous-même. Téléchargez le guide d'évaluation sur **www.attachmate.com/products/mss/mss-eval-form.html** ou contactez votre représentant commercial.

Pour en savoir plus, rendez-vous sur
www.microfocus.com/opentext

Communiquez avec nous

Blog du PDG d'OpenText Mark Barrenechea

262-FR0064-001 | O | 05/23 | © 2023 Open Text

opentext™