L’intégration du pare-feu de nouvelle génération dans l’environnement Citrix et Terminal Services

Eliminer les zones d’ombre et fournir une identité utilisateur sur le pare-feu dans un environnement client léger

Synthèse technique

Publication : Novembre 2012

Votre pare-feu créé-t-il des zones d'ombre dans la sécurité de votre environnement Citrix XenApp ou Microsoft Terminal Services ?

Dans la plupart des entreprises, les applications Windows sont installées localement, codées physiquement sur chaque machine, ce qui augmente leur coût de maintenance et de mise à jour.
Les applications qui sont fréquemment mises à jour, rarement utilisées ou difficiles à gérer deviennent problématiques pour les directions informatiques. Les entreprises comptant de nombreux utilisateurs ont tout à gagner en simplifiant la gestion de leurs applications.

Désormais, deux technologies très largement utilisées, Microsoft Terminal Services (rebaptisé Remote Desktop Services dans Windows Server 2008) et Citrix XenApp Server, permettent la mise à disposition d'applications virtuelles dans les entreprises comptant de nombreux employés géographiquement dispersés. Dans ces deux solutions, chaque application n'est packagée qu'une seule fois, pour être ensuite stockée sur un serveur ou un hub centralisé, au sein du datacenter. L'utilisateur peut exécuter l'application ou y accéder à partir de son poste « client léger ». Les programmes installés s'exécutent à partir d'un serveur central, ce qui rend inutile la mise à jour des programmes sur chaque poste distant. Ce type de solutions permet en outre de réduire la quantité de bande passante réseau nécessaire pour accéder aux programmes.

Citrix indique que *« XenApp délivre des applications sous forme de services à n'importe quel utilisateur, sur tout périphérique, quelle que soit sa localisation. »*[1]

La figure 1 présente un environnement typique, au sein duquel les utilisateurs accèdent aux applications à partir de clients légers géographiquement dispersés. Dans de nombreux cas, ces applications génèrent des appels vers un réseau protégé par un pare-feu XTM de WatchGuard.

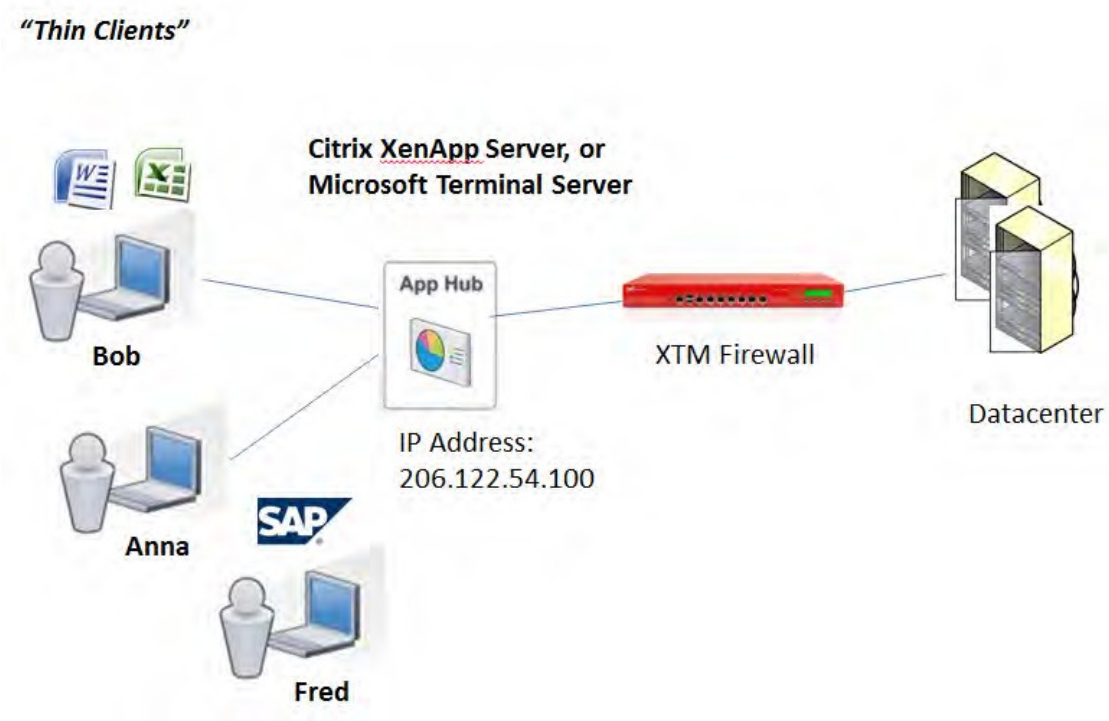


Figure 1 : Environnement typique au sein duquel les utilisateurs accèdent aux applications à partir de clients légers géographiquement dispersés.

Dans l'exemple ci-dessus, Fred, un utilisateur travaillant au siège de l'entreprise, doit remplir un formulaire de dépense via SAP. Fred utilise un Mac à la maison et un PC au bureau. Fred n'a pas besoin d'avoir SAP installé sur l'un de ces deux clients. SAP est tout simplement mis à la disposition de Fred sous la forme d'une application virtuelle hébergée dans un environnement virtuel sur le serveur XenApp. Fred interagit avec l'application exactement comme si celle-ci s'exécutait localement sur son poste de travail.

Tout comme Fred, les différents utilisateurs peuvent accéder aux programmes qui s'exécutent sur le hub d'applications (Citrix XenApp, Microsoft Remote Desktop ou Terminal Server) à partir de périphériques variés (ordinateurs personnels, bornes, matériels de faible puissance, etc.) et sur des systèmes d'exploitation autres que Windows.

L'idée paraît excellente. Alors, où est le problème ?

Les pare-feu traditionnels permettent de limiter l'accès à un réseau en établissant des règles pour les ports, les protocoles et les adresses IP. Pour le pare-feu, le trafic transitant par le serveur XenApp central semble provenir d'un seul client disposant de l'adresse IP du hub d'applications.

Lorsque de multiples utilisateurs se connectent à votre hub d'applications (Terminal Server ou serveur Citrix), puis se connectent à votre réseau ou à Internet, il peut s'avérer difficile de contrôler et d'assurer le suivi de ce trafic en fonction des noms d'utilisateurs ou de l'appartenance à un groupe.

Lorsque Bob (voir figure 1) s'authentifie sur le pare-feu, ce dernier l'associe à l'adresse IP du hub d'applications. Puis, lorsqu'Anna utilise une application et génère du trafic à partir de l'adresse IP du hub d'applications, le pare-feu identifie ce trafic comme provenant également de Bob. Le pare-feu ne peut pas distinguer parmi les différents utilisateurs connectés simultanément à votre hub d'applications lesquels génèrent réellement du trafic.

Eviter les zones d'ombre sécuritaires grâce aux solutions WatchGuard

WatchGuard résout ce problème grâce à l'installation du logiciel Terminal Services Agent sur le serveur utilisé comme hub d'applications. Lorsqu'un utilisateur se connecte au domaine, Terminal Services Agent recueille les informations relatives à l'utilisateur (authentifiant, groupe, nom de domaine) à partir de l'événement de connexion Windows et les transmet au périphérique XTM. Le périphérique XTM créé la session d'authentification pour l'utilisateur sur le pare-feu et transmet l'identifiant de session utilisateur à Terminal Services Agent. L'utilisateur n'a pas à s'authentifier manuellement sur le portail d'authentification, il bénéficie d'une expérience en « single sign-on » (SSO) totalement transparente. Lorsque l'utilisateur se déconnecte, Terminal Services Agent transmet automatiquement les informations de déconnexion au périphérique XTM, qui clôt la session authentifiée pour cet utilisateur.

Grâce au SSO pour Terminal Services, les utilisateurs n'ont plus à s'authentifier manuellement sur le portail d'authentification. Les utilisateurs qui se sont connectés via Terminal Services peuvent toutefois toujours s'authentifier manuellement. L'authentification manuelle prévaut toujours sur l'authentification SSO.

Les pare-feu de nouvelle génération : des noms et non plus des numéros, des utilisateurs et non plus des adresses IP

Les pare-feu de nouvelle génération permettent aux administrateurs d'établir des règles basées sur les noms d'utilisateur et non plus sur des concepts abstraits comme l'adresse IP.

Grâce à WatchGuard, les utilisateurs peuvent s'authentifier manuellement sur le pare-feu ou bénéficier du SSO, configurable via Active Directory. Le système d'exploitation des XTM permet en outre l'intégration de serveurs d'authentification tiers comme LDAP, Radius ou SecureID.

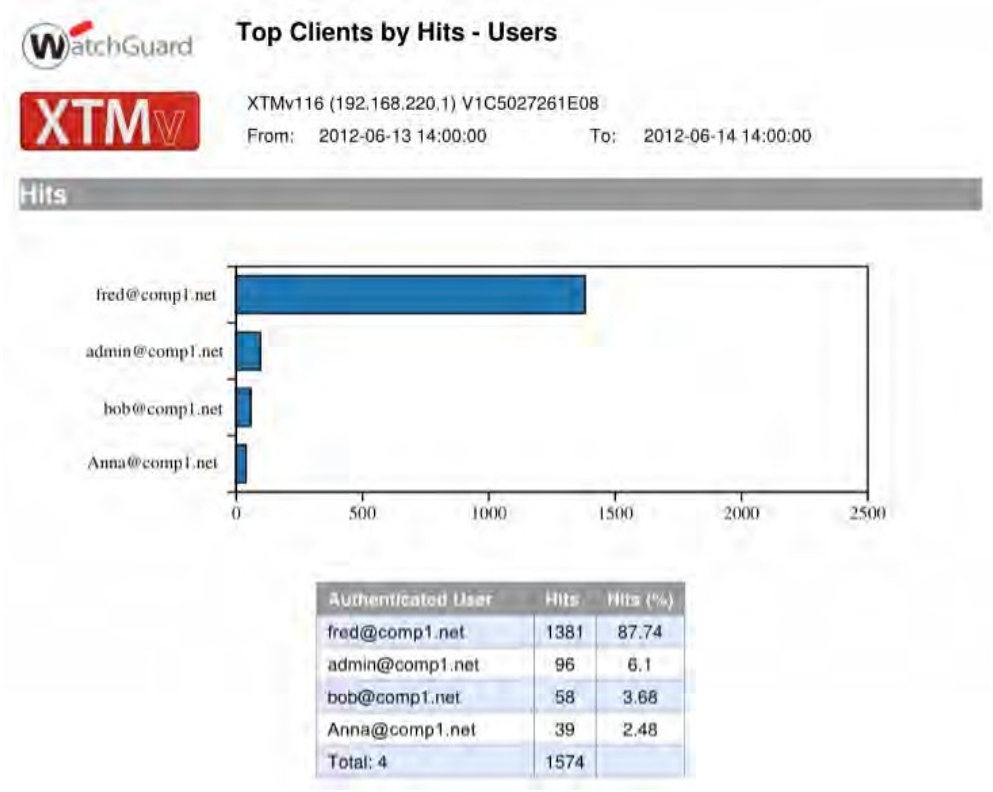
Les administrateurs peuvent créer des stratégies de pare-feu afin de permettre aux utilisateurs et aux groupes d'accéder à des ressources réseau spécifiques. Ce concept basé sur les utilisateurs au lieu des adresses IP s'applique également lorsque les utilisateurs accèdent à leurs applications dans des environnements Citrix ou Microsoft Terminal Services.

Les appliances XTM de WatchGuard incluent gratuitement plus de 65 rapports prédéfinis, qui fournissent des informations du niveau de l'utilisateur ou du client.

Quelques rapports prédéfinis proposés aux administrateurs :

- Applications ouvertes par les utilisateurs
- Principaux utilisateurs de bande passante
- Domaines et URL visités par les utilisateurs
- Applications inappropriées ou bloquées ouvertes par chaque utilisateur

Les rapports WatchGuard offrent des informations riches et détaillées, bien au-delà des simples adresses IP, et fournissent une visibilité jusqu'au niveau de l'utilisateur.



Authenticated User	Hits	Hits (%)
fred@comp1.net	1381	87.74
admin@comp1.net	96	6.1
bob@comp1.net	58	3.68
Anna@comp1.net	39	2.48
Total: 4	1574	

Figure 2 : Le compte-rendu du pare-feu affiche des informations relatives à l'utilisateur.

Remarque : Dans de nombreux pays européens, les règlementations en matière de confidentialité restreignent la capacité des entreprises à recueillir et conserver des informations relatives à l'activité de chaque utilisateur sur le réseau.

Le niveau de suivi des rapports du pare-feu XTM de WatchGuard est totalement configurable.

Versions compatibles :

La prise en charge de Terminal Services avec authentification manuelle ou en SSO fonctionne dans les environnements Citrix XenApp 4.5, 5.0, 6.0 et 6.5 ou Microsoft Terminal Services.

Documentation associée :

1. Citrix. « Guide des meilleures pratiques pour Provisioning Services et XenApp. » Livre blanc : http://support.citrix.com/servlet/KbServlet/download/19542-102-665106/PVS%20-%20PVS%20for%20XenApp%20Best%20Practices.pdf
2. Citrix : http://www.citrix.com/products/xenapp/how-it-works.html#video-launcher-lightbox-3650235
3. Microsoft : Présentation de Remote Desktop Services (Terminal Services) : http://technet.microsoft.com/en-us/library/cc725560.aspx
4. Documentation utilisateur WatchGuard (rechercher « Terminal Services » : http://www.watchguard.com/help/docs/wsm/11_XTM/en-US/index.html

Pour en savoir plus

Pour en savoir plus, visitez le site Web de WatchGuard, contactez un revendeur WatchGuard, ou appelez le 01 47 90 30 35

ADRESSE :
La Grande Arche, Paroi Nord
92044 Paris La Defense

A PROPOS DE WATCHGUARD

Depuis 1996, WatchGuard Technologies fournit des appliances de sécurité fiables et simples à gérer à des centaines de milliers d'entreprises dans le monde. Les solutions de sécurité réseau WatchGuard XTM, plusieurs fois récompensées, associent des services VPN, de pare-feu et de sécurité. Les appliances XCS garantissent la sécurité des contenus sur les messageries et le Web, ainsi que la prévention des pertes de données. Ces deux lignes de produits vous aident à atteindre vos objectifs de conformité réglementaire. Plus de 15 000 partenaires représentent WatchGuard dans 120 pays. Le siège de WatchGuard est basé à Seattle, dans l'état de Washington, et l'entreprise compte de nombreux bureaux en Amérique du Nord, en Amérique Latine, en Europe et dans la zone Asie-Pacifique. Pour en savoir plus, visitez www.watchguard.com.