# Comment le traitement Skype des appareils de sécurité Web de Cisco (WSA) trafique-t-il ?

## Contenu



## Question :

Comment le traitement Skype des appareils de sécurité Web de Cisco (WSA) trafique-t-il ?

**Environnement :** Cisco WSA, Skype

Skype est un réseau de propriété industrielle de la téléphonie Internet (VoIP). Skype fonctionne principalement comme programme peer-to-peer, ainsi il ne communique pas directement avec un serveur central pour fonctionner. Il peut être particulièrement difficile bloquer Skype, car il tentera de se connecter de beaucoup de différentes manières.

Skype se connecte dans l'ordre de préférence suivant :

1. Paquets UDP directs à d'autres pairs à l'aide des numéros de port aléatoires
2. Paquets TCP directs à d'autres pairs à l'aide des numéros de port aléatoires
3. Paquets TCP directs à d'autres pairs utilisant le port 80 et/ou le port 443
4. Les paquets percés un tunnel par l'intermédiaire d'un proxy de Web utilisant un HTTP SE CONNECTENT au port 443

Quand déployé dans un environnement explicite de proxy, des méthodes 1-3 ne seront jamais envoyées à Cisco WSA. Afin de bloquer Skype, il doit d'abord être bloqué d'un autre emplacement dans le réseau. Étapes de Skype 1-3 peuvent être bloquées utilisant :

- Pare-feu : Utilisation NBAR de bloquer la version 1 de Skype. Plus d'informations sont disponibles chez http://ciscotips.wordpress.com/2006/06/07/how-to-block-skype/
- Cisco IPS (ASA) : Cisco ASA peut potentiellement détecter et bloquer Skype par l'intermédiaire des signatures.

Quand Skype retombe à utiliser un proxy explicite, Skype ne fournit délibérément aucun petit groupe de client dans la requête de connexion de HTTP (aucune chaîne d'utilisateur-agent non plus). Ceci le rend difficile à différencier entre Skype et une requête de connexion valide. Skype se connectera toujours au port 443 et l'adresse de destination est toujours une adresse IP.

*Exemple :*

CONNECTEZ 10.129.88.111:443 HTTP/1.0
Proxy-connexion : keep-alive

La stratégie suivante d'Access bloquera toutes les requêtes de connexion par le WSA qui apparie

les adresses IP et le port 443. Ceci appariera tout le trafic de Skype. Cependant, des programmes de non-Skype essayant de percer un tunnel à une adresse IP sur le port 443 seront aussi bien bloqués.

### Bloquant Skype - Environnement explicite avec le proxy HTTPS désactivé

Créez une catégorie URL de coutume pour apparier le trafic IP et de port 443 :

1. Naviguez vers le « directeur de la sécurité » - > « des catégories faites sur commande URL » - > « ajoutent la catégorie faite sur commande ».
2. Complétez le « nom de catégorie » et développez « a avancé ».
3. Utilisation "[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+" dans la fenêtre d'expression régulière.

Placez cette catégorie pour refuser dans les stratégies d'Access :

1. Naviguez vers le « gestionnaire de sécurité Web » - > des « stratégies d'Access ».
2. Cliquez sur le lien sous la colonne « de catégories URL » pour le policy group compétent.
3. Dans la section de filtrage « de catégorie faite sur commande URL », choisissez le « bloc » pour la nouvelle catégorie de Skype.
4. Soumettez et commettez les modifications

*Remarque:* Des requêtes de connexion explicites peuvent seulement être bloquées si le service proxy HTTPS est désactivé !

Quand le déchiffrement WSA HTTPS est activé, le trafic de Skype peut très probablement se casser parce que ce n'est pas purement le trafic HTTPS (l'outrage utilisant SE CONNECTENT et le port 443). Ceci aura comme conséquence une erreur 502 générée par le WSA et la connexion sera abandonnée. N'importe quel vrai trafic web HTTPS à une adresse IP continuera à fonctionner (bien qu'il sera déchiffré sur le WSA).

### Bloquant Skype - Environnement explicite/transparent avec le proxy HTTPS activé

Créez une catégorie faite sur commande pour apparier le trafic IP et de port 443 :

1. Naviguez vers le « directeur de la sécurité » - > « des catégories faites sur commande URL » - > « ajoutent la catégorie faite sur commande ».
2. Complétez le « nom de catégorie » et développez « a avancé ».
3. Utilisation "[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+" dans la fenêtre d'expression régulière.

Placez cette catégorie pour déchiffrer dans les stratégies de déchiffrement :

1. Naviguez vers le « gestionnaire de sécurité Web » - > des « stratégies de déchiffrement ».
2. Cliquez sur le lien sous la colonne « de catégories URL » pour le policy group compétent.
3. Dans la section de filtrage « de catégorie faite sur commande URL », choisissez le « déchiffrage » pour la nouvelle catégorie de Skype.
4. Soumettez et commettez les modifications.

*Remarque:* Puisque le trafic de Skype est envoyé à un IP, il sera considéré en tant qu'élément « de l'URLs Uncategorized ». Le même effet comme ci-dessus se produira selon si l'action doit déchiffrer ou fonction émulation.