Contenu

Question :

Que les différents codes de réponse de HTTP signifient-ils ?

Environnement : Appliance de sécurité Web de Cisco (WSA) exécutant toute version d'AsyncOS

Le HTTP a toujours une demande de client et une réponse de serveur. Les réponses de serveur sont classifiées par un code numérique de réponse. Les codes de réponse indiquent les raisons derrière des demandes de HTTP réussies et défectueuses.

Pour les pleines informations détaillées concernant des codes de réponse de HTTP, voir s'il vous plaît le RFC 2616 (HTTP), la section 10.

Sont ci-dessous les détails concernant le code de réponse le plus commun que vous êtes susceptible de s'exécuter dans :

codes **1xx** : Informationnel

100 continuent : Typiquement vu en vue de le protocole ICAP. C'est une réponse informationnelle qui nous font le client savoir qu'elle peut continuer à envoyer des données. En vue de des services ICAP (tels que la lecture de virus), le serveur peut seulement vouloir voir la première quantité x d'octets. Quand il est fait balayant le premier ensemble d'octets et n'a pas détecté un virus, il enverra des 100 continuent à faire le client savoir pour envoyer le reste de l'objet.

codes **2xx** : Réussi

OK 200 : Le code de réponse le plus commun. Ceci signifie que la demande est réussie sans problème.

codes 3xx : Redirection

302 trouvé : C'est une redirection provisoire. Le client est chargé de faire une nouvelle demande de l'objet spécifié dans l'emplacement : en-tête.

304 non modifié : C'est en réponse à un **GIMS** (OBTENEZ Si-modifier-puisque). C'est littéralement un HTTP standard OBTIENNENT qui inclut l'en-tête Si-modifier-**puisque : <date>.** Cette en-tête indique au serveur que le client a une copie de l'objet prié dans lui est cache local et incluse est la date où l'objet a été cherché. Si l'objet a été modifié depuis cette date, le serveur répondra avec un OK 200 et une copie fraîche de l'objet. Si l'objet n'a pas changé puisque la date cherchée, le serveur renverra une réponse 304 non modifiée.

307 provisoire réorientez : À toutes fins utiles, il a la même signification que les 302. Si d'autres détails sont découverts, cet article peut être mis à jour.

codes 4xx : Erreur de client

Mauvaise demande 400 : Ceci signifie que la quelque chose dans la demande de HTTP n'est pas syntaxe appropriée suivante. Les causes possibles ont pu être dues à de plusieurs en-têtes étant sur la même ligne, les espaces dans une en-tête, aucun HTTP/1.1 dans l'URI, tellement en avant. RFC 2616 devrait être mis en référence pour la syntaxe appropriée.

401 non autorisé : L'objet demandé exige de l'authentification afin de pour être accédé à. Les 401 est utilisés pour l'authentification à un web server de destination. En utilisant l'appliance de sécurité Web de Cisco (WSA) dans le mode transparent, des 401 est renvoyés au client quand l'authentification est activée sur le proxy. C'est parce que l'appliance se charrie comme si c'étaient l'OCS (serveur de contenu d'origine).

Les méthodes d'authentification disponibles sont spécifiées dans un WWW-**authentifier** : En-tête de réponse de HTTP. Ceci indiquera au client si ce serveur demande NTLM, de base, ou d'autre méthode d'authentification.

403 interdit : Le client est refusé d'accéder à l'objet prié. Il y a beaucoup de causes pour pourquoi un serveur peut refuser l'accès à un objet. Typiquement, le serveur inclura un certain tri de la description de la cause dans les données de HTTP (réponse HTML).

404 non trouvé : L'objet demandé n'existe pas sur le serveur.

Authentification de proxy 407 requise : C'est identique que des 401, sauf qu'il est spécifiquement pour l'authentification à un proxy, pas l'OCS. Ceci est envoyé seulement si la demande était envoyée explicitement au proxy. Des 407 ne peuvent pas être envoyés à un client tout en utilisant WSA en tant que proxy transparent, en tant que client ne sait pas que le proxy existe. Si c'est le cas, le client très probablement FIN ou RST le socket de TCP.

Au lieu de l'utilisation WWW-authentifiez : en-têtes pour spécifier quelles méthodes d'authentification sont disponibles, le proxy-**authentifier** : l'en-tête est utilisée.

codes 5xx : Erreur du serveur

Erreur interne du serveur 500 : Panne générique de serveur

Passerelle du mauvais 502 : Vous verrez typiquement ceci quand utilisant le WSA comme proxy, où la passerelle répond inexactement.

Service 503 indisponible : Ceci est typiquement envoyé quand l'OCS est au-dessus d'encombrer. Tenter la demande de nouveau à une date ultérieure devrait être réussi.

Délai d'attente de 504 passerelles : Des 504 seront envoyés si WSA ne recevait pas une réponse de sa passerelle.