Question de filtre du trafic de BotNet avec l'appliance de sécurité adaptable

Contenu

Introduction

Ce document décrit les étapes pour dépanner la fonctionnalité de filtre du trafic de BotNet sur l'appliance de sécurité adaptable (ASA). Pour l'assistance avec la configuration de filtre du trafic de BotNet, voir le ce ce guide de configuration : Configurer le filtre du trafic de BotNet.

Informations générales

Les demandes et les réponses de Domain Name Server de moniteurs de filtre du trafic de BotNet (DN) entre les clients DNS internes et les serveurs DNS externes. Quand une réponse de DN est traitée, le domaine associé avec la réponse est vérifié contre la base de données des domaines malveillants connus. S'il y a une correspondance, promouvez le trafic à l'adresse IP actuelle dans les DN que la réponse est bloquée. Voir le ce diagramme.

1. **Vérifiez la base de données dynamique de filtre.** L'ASA télécharge périodiquement une base de données en cours des domaines et des IP address malveillants connus. Les exécutions de renseignements de sécurité de Cisco (SIO) détermine que les domaines et les adresses IP dans cette base de données servent le malware ou tout autre contenu malveillant.
2. **Assurez-vous que le trafic DNS croise l'ASA.** Un utilisateur sur le réseau interne ou un ordinateur infecté sur les essais de réseau interne pour accéder à un serveur malveillant afin de télécharger le malware ou participer à un BotNet. Afin de se connecter au serveur malveillant, l'ordinateur hôte doit exécuter une consultation de DN. Dans cet exemple, l'accès de tentatives d'ordinateur à badsite.cisco.com. L'ordinateur hôte envoie une demande de DN à un serveur DNS local ou directement à un serveur DNS externe. Dans les deux situations, une demande de DN doit traverser l'ASA et la réponse de DN doit également traverser la même ASA.
3. **Vérifiez le cache de Dn-fureteur.** La fonction de Dn-fureteur de l'inspection de DN, si activée, surveille le trafic DNS et détermine qu'une réponse d'Un-enregistrement de DN est retournée

du serveur DNS. La fonction de Dn-fureteur prend le domaine et les adresses IP actuels dans la réponse d'Un-enregistrement et les ajoute au cache de Dn-fureteur. Le domaine est vérifié contre la base de données téléchargée de l'étape 1 et une correspondance est trouvée. La réponse de DN n'est pas abandonnée et est permise pour traverser.

4. **Testez le filtre du trafic de BotNet avec le trafic.** Puisqu'il y avait une correspondance dans l'étape 3, l'ASA ajoute une règle interne qui indique que tout le trafic à ou de l'IP associé avec badsite.cisco.com est relâché. Les essais infectés d'ordinateur puis pour accéder au serveur et le trafic URL badsite.cisco.com est abandonnés.

Dépannez le processus

Employez ces étapes afin de dépanner et vérifier que la caractéristique fonctionne.

Étape 1 : Vérifiez la base de données dynamique de filtre

Vérifiez si la base de données l'a téléchargé et saisissez les **données de dynamique-filtre d'exposition de** commande. Voir la cette sortie témoin :

```
# show dynamic-filter data
Dynamic Filter is using downloaded database version '1404865586'
Fetched at 21:32:02 EDT Jul 8 2014, size: 2097145
Sample contents from downloaded database:
dfgdsfgsdfg.com bulldogftp.com bnch.ru 52croftonparkroad.info
paketoptom.ru lzvideo.altervista.org avtovirag.ru cnner.mobi
Sample meta data from downloaded database:
threat-level: very-high, category: Malware,
description: "These are sources that use various exploits to deliver adware,
spyware and other malware to victim computers. Some of these are associated
with rogue online vendors and distributors of dialers which deceptively
call premium-rate phone numbers." threat-level: high, category: Bot
and Threat Networks, description: "These are rogue systems that
control infected computers. They are either systems hosted on
threat networks or systems that are part of the botnet itself
threat-level: moderate, category: Malware,
description: "These are sources that deliver deceptive or malicious anti-spyware,
anti-malware, registry cleaning, and system cleaning software."
threat-level: low, category: Ads,
description: "These are advertising networks that deliver banner ads,
interstitials, rich media ads, pop-ups, and pop-unders for websites,
spyware and adware. Some of these networks send ad-oriented HTML emails
and email verification services."
Total entries in Dynamic Filter database:
Dynamic data&colon; 80677 domain names , 4168 IPv4 addresses
Local data&colon; 0 domain names , 0 IPv4 addresses
Active rules in Dynamic Filter asp table:
Dynamic data&colon; 0 domain names , 4168 IPv4 addresses
Local data&colon; 0 domain names , 0 IPv4 addresses
```

Dans cette sortie, l'ASA indique la période du dernier effort réussi de base de données et un échantillon du contenu dans cette base de données. Si vous vous exécutez les **données de dynamique-filtre d'exposition de** commande, et la commande prouve qu'aucune base de données ne l'a téléchargé, dépannent cette étape d'abord. Les problèmes courants qui empêchent l'ASA d'obtenir la base de données dynamique de filtre incluent :

- **Configuration DNS manquante ou incorrecte sur l'ASA.** Le client dynamique d'updater de filtre

doit résoudre le nom d'hôte du serveur de mise à jour. Les DN doivent être configurés et fonctionnels sur l'ASA. Cinglez les domaines réputés de la ligne de commande et déterminez si l'ASA peut résoudre des adresses Internet.

- **Aucun accès Internet de l'ASA.** Si l'ASA est sur un réseau qui n'a pas accès à l'Internet, ou un périphérique en amont bloque les ASA en dehors de l'adresse IP de l'accès à l'Internet, la mise à jour échoue.
- **Le client d'Updater n'est pas activé**. **L'enable d'Updater-client de dynamique-filtre de** commande doit être configuré de sorte que l'ASA puisse télécharger la base de données.

Sélectionnez la commande **mettent au point l'Updater-client de dynamique-filtre** afin de mettre au point la base de données. Voir la cette sortie témoin de la commande :

```
Dynamic Filter: Updater client fetching dataDynamic Filter: update
startingDBG:01:2902417716:7fff2c33ec28:0000: Creating fiber
0x7fff2c4dce90 [ipe_request_fiber], stack(16384) =
0x7fff2c505c60..0x7fff2c509c58 (fc=2),
sys 0x7fff20906038 (FIBERS/fibers.c:fiber_create:544)
DBG:02:2902417779:7fff2c4dce90:0000: Jumpstarting ipe_request_fiber 0x7fff2c4dce90,
sys 0x7fff2c33eba0 (FIBERS/fibers-jumpstart.c:_fiber_jumpstart:36)
Dynamic Filter: Created lua machine, launching lua script
DBG:03:2902422654:7fff2c4dce90:0000: Connecting to 00000000:1591947792
(SAL/netsal.c:netsal_client_sock_connect:323)
DBG:04:2902422667:7fff2c4dce90:0000: otherPifNum 3, nexthop4 17c12ac
(SAL/netsal.c:netsal_client_sock_connect:374)
DBG:05:2902422691:7fff2c4dce90:0000: about to call netsal__safe_encapsulate for
(sal-np/ssl/CONNECT/3/208.90.58.5/443/M/0/NOTUNGW)
(SAL/netsal.c:netsal_client_sock_connect:446)
DBG:06:2902422920:7fff2c4dce90:0000: connection timeout set for 10 seconds
(SAL/netsal.c:netsal_client_sock_connect:473)
DBG:07:2902750615:7fff2c4dce90:0000: SALNPCLOSENOTIFY: p=0x0 0/0 more buffered
(SAL/channel-np.c:_sal_np_ioctl:1312)
Dynamic Filter: Processing updater server response
Dynamic Filter: update file url1 =
http://updates.ironport.com/threatcast/1.0/blacklist/2mb-1file/1404865586
Dynamic Filter: update file url2 =
http://updates.ironport.com/threatcast/1.0/blacklist/2mb-1file/1404865586
Channel NP p=0x0000000000000000 0/0 more bufferedchannel-np.cDBG:08:2902784011:
7fff2c4dce90:0000: Connecting to 00000000:538976288
(SAL/netsal.c:netsal_client_sock_connect:323)
DBG:09:2902784026:7fff2c4dce90:0000: otherPifNum 3, nexthop4 17c12ac
(SAL/netsal.c:netsal_client_sock_connect:374)
DBG:10:2902784051:7fff2c4dce90:0000: about to call netsal__safe_encapsulate for
(sal-np/tcp/CONNECT/3/208.90.58.25/80/M/0/NOTUNGW)
(SAL/netsal.c:netsal_client_sock_connect:446)
DBG:11:2902784241:7fff2c4dce90:0000: connection timeout set for 10 seconds
(SAL/netsal.c:netsal_client_sock_connect:473)
DBG:12:2902914651:7fff2c4dce90:0000: SALNPCLOSENOTIFY: p=0x0 0/0 more buffered
(SAL/channel-np.c:_sal_np_ioctl:1312)
DBG:13:2902914858:7fff2c4dce90:0000: Connecting to 00000000:25465757
(SAL/netsal.c:netsal_client_sock_connect:323)
DBG:14:2902914888:7fff2c4dce90:0000: otherPifNum 3, nexthop4 17c12ac
(SAL/netsal.c:netsal_client_sock_connect:374)
DBG:15:2902914912:7fff2c4dce90:0000: about to call netsal__safe_encapsulate for
(sal-np/tcp/CONNECT/3/208.90.58.25/80/M/0/NOTUNGW)
(SAL/netsal.c:netsal_client_sock_connect:446)
DBG:16:2902915113:7fff2c4dce90:0000: connection timeout set for 10 seconds
(SAL/netsal.c:netsal_client_sock_connect:473)
Channel NP p=0x0000000000000000 0/0 more bufferedchannel-np.cDBG:17:2907804137:
7fff2c4dce90:0000: SALNPCLOSENOTIFY: p=0x0 0/0 more buffered
(SAL/channel-np.c:_sal_np_ioctl:1312)
Dynamic Filter: Successfully downloaded the update file from url1
```

```
Dynamic Filter: Successfully finished lua script
DBG:18:2907804722:7fff2c4dce90:0000: Fiber 0x7fff2c4dce90 finished leaving 3 more
(FIBERS/fibers-jumpstart.c:_fiber_jumpstart:64)
DBG:19:2907804746:7fff2c4dce90:0000: Exiting fiber 0x7fff2c4dce90
(FIBERS/fibers.c:fiber__kill:1287)
DBG:20:2907804752:7fff2c4dce90:0000: Fiber 0x7fff2c4dce90 terminated, 2 more
(FIBERS/fibers.c:fiber__kill:1358)
Dynamic Filter: Downloaded file successfully
Channel NP p=0x0000000000000000 0/0 more bufferedchannel-np.cDynamic Filter: read
ramfs bytes 2097152
Dynamic Filter: file MD5 verification check succeeded
Dynamic Filter: decrypt key succeeded
Dynamic Filter: decrypt file succeeded byte = 2097145
Dynamic Filter: updating engine bytes = 2097145
Dynamic Filter: meta data length = 2987
INFO: Dynamic Filter: update succeeded
```

Dans cette sortie, vous pouvez voir ces mesures que l'updater prend quand il obtient une nouvelle base de données :

- L'updater atteint à l'URL http://update-manifests.ironport.com afin de déterminer quelle base de données il télécharge.
- Le serveur manifeste renvoie deux URLs possible pour le téléchargement.
- Le client d'updater télécharge la base de données.
- La base de données est déchiffrée et enregistrée dans la mémoire à l'usage du procédé de filtration dynamique.

Les problèmes de connectivité pour différents serveurs de mise à jour se manifestent comme erreurs dans cette sortie et aident à dépanner plus loin. Forcez le client d'updater pour s'exécuter manuellement avec l'**effort dynamique de base de données de filtre de** commande.

Étape 2 : Assurez que le trafic DNS croise cette ASA

La fonctionnalité de filtre du trafic de BotNet de l'ASA est établie hors fonction des adresses IP qui apparient des domaines, ainsi l'ASA doit être en conformité avec les demandes et les réponses de DN qui traversent le réseau. Quelques topologies pourraient faire prendre le trafic DNS un chemin qui n'inclut pas l'ASA en question. La plupart des réseaux ont des serveurs DNS internes qui agissent en tant que dns forwarder et caches pour les usrs internes. Tant que ces serveurs, quand ils les expédient à une demande de DN d'un domaine ne possèdent pas ou ne peuvent pas répondre pour, font suivre à la demande un serveur qui a besoin de traverser l'ASA, aucun problème ne devrait se poser. Voir les ces topologies avec et sans des serveurs DNS internes :

Cet exemple de topologie affiche les utilisateurs qui indiquent un serveur DNS interne quel en avant à un serveur DNS externe.

Cet exemple de topologie affiche les utilisateurs qui indiquent directement un serveur DNS externe.

Dans les deux exemples de topologie, la clé à un déploiement fonctionnel de filtre du trafic de BotNet est que les demandes record des DN A des domaines externes doivent traverser l'ASA qui exécute la caractéristique de Dn-fureteur. Dans l'exemple de serveur interne, si le serveur DNS interne prend un chemin réseau différent afin d'atteindre l'Internet que l'ordinateur d'utilisateur, et dans le processus ne traverse pas l'ASA, la table de Dn-fureteur ne contiendra pas des cartes d'IP-à-domaine provoquées par des demandes de DN d'ordinateur d'utilisateur et l'ordinateur d'utilisateur ne pourrait pas être filtré comme prévu.

Employez ces techniques afin de vérifier que le trafic DNS traverse l'ASA :

- Vérifiez la service-stratégie. Regardez la sortie du **show service-policy** afin de déterminer si l'inspection de DN est appliquée, configuré avec le mot clé de dynamique-filtre-**fureteur**, et voyez le trafic. Le compte de paquet associé avec l'inspection de DN devrait incrémenter pendant que vous faites des demandes de DN.
- Captures d'utilisation. La caractéristique de Dn-fureteur regarde les paquets de DN qui traversent l'ASA, ainsi il est important que vous vérifiiez que les paquets atteignent l'ASA. Employez la fonction intégrée de la capture de l'ASA afin de s'assurer que le trafic DNS écrit et part de cette ASA correctement.

Étape 3 : Vérifiez le cache de fureteur de DN

la trésorerie de Dn-fureteur devrait la remplir avec des cartes d'IP-à-domaine. Une adresse IP simple pourrait avoir un nombre sans limites de domaines assocated avec elle. C'est comment les sociétés qui hébergent des sites Web peuvent servir des milliers de domaines avec juste quelques adresses IP. Présentez le **petit groupe de dn-fureteur de dynamique-filtre d'exposition de** commande et voyez le vidage mémoire des données actuellement dans le cache de Dn-fureteur. C'est un enregistrement de toutes les cartes d'IP-à-domaine que l'ASA obtient avec l'utilisation de la fonction de Dn-fureteur de l'inspection de DN. Voir la cette sortie témoin :

```
DNS Reverse Cache Summary Information: 3 addresses, 3 names
Next housekeeping scheduled at 22:28:01 EDT Jul 8 2014,
DNS reverse Cache Information:
[198.151.100.77] flags=0x1, type=0, unit=0 b:u:w=0:1:0, cookie=0x0
[cisco.com] type=0, ttl=31240
[198.151.100.91] flags=0x23, type=0, unit=0 b:u:w=1:1:0, cookie=0x0
[magnus.cisco.com] type=1, ttl=0
[raleigh.cisco.com] type=0, ttl=0
[198.151.100.1] flags=0x2, type=0, unit=0 b:u:w=1:0:0, cookie=0x0
[badsite.cisco.com] type=1, ttl=0
```

Dans cet exemple, l'ASA apprend des informations sur trois adresses IP mais quatre domaines. **magnus.cisco.com** et **raleigh.cisco.com** chacun des deux les résolvent à 198.151.100.91. Dans cet exemple, deux des domaines, **magnus.cisco.com** et **badsite.cisco.com** les répertorient comme type 1. Ceci signifie que le domaine est trouvé dans la base de données comme domaine mis sur la liste noire. Les autres domaines sont répertoriés comme type 0, qui indique que le domaine n'est pas mis ou whitelisted sur la liste noire et est juste un domaine normal.

1. Vérifiez que les demandes de DN d'un ordinateur d'utilisateur eventially traversent le Pare-feu et sont traitées par le Dn-fureteur et faites une demande de DN. Vérifiez le cache pour une entrée qui s'assortit. Testez et utilisez un domaine qui les résolutions mais est assez obscure qu'il n'a pas été questionné récemment et est déjà dans la table. Par exemple, le domaine asa.cisco.com est choisi. Le nslookup d'outil de ligne de commande est utilisé pour questionner cette adresse Internet. Reportez-vous à l’exemple suivant :

   ```
   $ nslookup asa.cisco.com

   Name: asa.cisco.com
   Address: 198.151.100.64
   ```

2. Vérifiez le cache de Dn-fureteur. Reportez-vous à l’exemple suivant :

   ```
   DNS Reverse Cache Summary Information: 5 addresses, 7 names
   Next housekeeping scheduled at 22:48:01 EDT Jul 8 2014,
   ```

```
DNS reverse Cache Information:
[198.151.100.64] flags=0x11, type=0, unit=0 b:u:w=0:1:0, cookie=0x0
[asa.cisco.com] type=0, ttl=86359
```

L'entrée est présente dans le cache de Dn-fureteur. Si l'entrée n'était pas présente avant que le test de nslookup, il signifie que les travaux de caractéristique de Dn-fureteur et que l'ASA fonctionne correctement avec des demandes et des réponses de DN.

Si l'entrée n'affiche pas, assurez-vous que le trafic DNS traverse l'ASA. Vous pourriez devoir vider le cache DNS sur l'ordinateur hôte ou les serveurs DNS internes, si c'est approprié, afin de s'assurer que des demandes ne sont pas servies d'un cache.

La caractéristique de Dn-fureteur ne prend en charge pas EDNS0. Si le client DNS ou le serveur utilise EDNS0, l'ASA ne pourrait pas remplir cache de Dn-fureteur en présence des cartes d'IP-à-domaine si la réponse a des enregistrements de ressource supplémentaire. Cette limite est dépistée par l'ID de bogue Cisco CSCta36873.

Étape 4 : Testez le filtre du trafic de BotNet avec le trafic

Dans l'étape 3, le cache de Dn-fureteur prouve que le domaine badsite.cisco.com est sur la liste noire. Cinglez le domaine en question afin de tester la fonctionnalité de botnet. Quand vous cinglez le le domaine, il est plus sûr que si vous essayez de charger le domaine dans un navigateur Web. Ne testez pas la caractéristique dynamique de filtre à l'aide de votre navigateur Web parce que votre ordinateur pourrait être compromis si le navigateur charge le contenu malveillant. Utilisez le Protocole ICMP (Internet Control Message Protocol) parce que c'est une méthode plus sûre et est un test valide du filtre du trafic de BotNet car il bloque basé sur l'IP et rien spécifiques pour mettre en communication ou le protocole.

Si vous ne savez pas d'un site mis sur la liste noire, vous pouvez trouver un facilement. Écrivez le **<search_term> de découverte de base de données de dynamique-filtre de** commande pour trouver les domaines qui sont mis sur la liste noire et pour apparier le terme à rechercher fourni. Reportez-vous à l'exemple suivant :

```
ASA# dynamic-filter database find cisco verybadsite.cisco.com
m=44098 acmevirus.cisco.com m=44098Found more than 2 matches,
enter a more specific string to find an exact match
```

Ping un des domaines qui retourne. Quand vous cinglez ce domaine, il entraînera ces actions de se produire :

1. L'hôte génère une demande de DN du domaine en question.
2. La demande de DN traverse l'ASA, directement de l'ordinateur hôte ou expédié par un serveur interne.
3. La réponse de DN traverse l'ASA, de nouveau à l'ordinateur hôte ou au serveur interne.
4. La fonction de Dn-fureteur remplit cette carte d'IP-à-domaine dans le cache de Dn-fureteur.
5. L'ASA compare le domaine contre la base de données de dyanmic-filtre et détermine une correspondance. L'ASA bloque davantage de trafic en entrée et en sortie de l'IP associé avec le domaine malveillant.
6. L'ordinateur hôte envoie à une requête d'écho d'ICMP cette les baisses ASA parce qu'il est destiné à un IP associé avec un domaine malveillant.

Quand l'ASA relâche le trafic de test d'ICMP, elle se connecte un log système (Syslog) semblable à cet exemple :

```
Jul 08 2014 23:14:17: %ASA-4-338006: Dynamic Filter dropped blacklisted
ICMP traffic from inside:192.168.1.100/23599 (203.0.113.99/23599) to
outside:198.151.100.72/0 (198.151.100.72/0), destination 198.151.100.72
resolved from dynamic list: acmevirus.cisco.com, threat-level: very-high,
category: Malware
```

La sortie des **statistiques de dynamique-filtre d'exposition de** commande indique les connexions qui sont classifiées et potentiellement abandonnées. Reportez-vous à l'exemple suivant :

```
ASA(config)# show dynamic-filter statistics
Enabled on interface inside
Total conns classified 163, ingress 163, egress 0
Total whitelist classified 0, ingress 0, egress 0
Total greylist classified 8, dropped 0, ingress 8, egress 0
Total blacklist classified 155, dropped 154, ingress 155, egress 0
Enabled on interface outside
Total conns classified 0, ingress 0, egress 0
Total whitelist classified 0, ingress 0, egress 0
Total greylist classified 0, dropped 0, ingress 0, egress 0
Total blacklist classified 0, dropped 0, ingress 0, egress 0
Enabled on interface management
Total conns classified 0, ingress 0, egress 0
Total whitelist classified 0, ingress 0, egress 0
Total greylist classified 0, dropped 0, ingress 0, egress 0
Total blacklist classified 0, dropped 0, ingress 0, egress 0
```

Le compteur classifié augmente seulement si une tentative de connexion est faite à une adresse IP qui est mise, whitelisted sur la liste noire, ou greylisted. Tout autre trafic n'entraîne pas classifié à l'opposé de l'augmentation. Un nombre peu élevé pour la liste classifiée ne signifie pas que l'ASA n'a pas évalué de nouvelles tentatives de connexion contre le filtre du trafic de BotNet. Ce nombre peu élevé indique à la place que peu des adresses IP de source ou de destination sont mises, whitelisted sur la liste noire, ou greylisted. Employez les instructions dans ce document afin de confirmer les fonctions de caractéristique correctement.

Si le trafic de test n'est pas abandonné, vérifiez la configuration afin de s'assurer qu'elle est configurée pour relâcher le trafic avec un niveau approprié de menace. Voir la cette configuration d'échantillon, qui active le filtre du trafic de BotNet globalement sur l'ASA ici :

```
dynamic-filter updater-client enable
dynamic-filter use-database
dynamic-filter enable
dynamic-filter drop blacklist
```