Configuration de la détection des menaces pour les services VPN d'accès à distance sur Secure Firewall ASA

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Configurer

- Détection des menaces pour les tentatives de connexion à des services VPN internes uniquement (non valides)
- Détection des menaces pour les attaques d'initiation du client VPN d'accès distant
- Détection des menaces pour les échecs d'authentification VPN d'accès à distance

Vérifier

Informations connexes

Introduction

Ce document décrit le processus de configuration des fonctionnalités de détection des menaces pour le VPN d'accès à distance sur Cisco Secure Firewall ASA.

Conditions préalables

Exigences

Cisco vous recommande d'avoir des connaissances sur les sujets suivants :

- Appareil de sécurité adaptatif Cisco Secure Firewall (ASA)
- VPN d'accès à distance (RAVPN) sur ASA

Ces fonctions de détection des menaces sont prises en charge dans les prochaines versions de Cisco Secure Firewall ASA :

- version 9.16 train > prise en charge à partir de la version 9.16(4)67 et des versions plus récentes de cette série spécifique.
- version 9.17 train > prise en charge à partir de la version 9.17(1)45 et des versions plus récentes dans ce train spécifique.
- version 9.18 de train > prise en charge à partir de la version 9.18(4)40 et des versions plus récentes de ce train spécifique.
- version 9.19 train > prise en charge à partir de la version 9.19(1).37 et des versions plus récentes de cette série spécifique.
- version 9.20 de train > prise en charge à partir de la version 9.20(3) et des versions plus récentes de ce train spécifique.
- version 9.22 train > prise en charge à partir de la version 9.22(1.1) et des versions ultérieures.

Note : 9.22(1) n'a pas été publié. La première version était 9.22(1.1).

Composants utilisés

Les informations décrites dans ce document sont basées sur les versions matérielles et logicielles suivantes :

- Cisco Secure Firewall ASA version 9.20(3)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Les fonctionnalités de détection des menaces pour les services VPN d'accès à distance permettent d'empêcher les attaques par déni de service (DoS) à partir d'adresses IPv4 en bloquant automatiquement l'hôte (adresse IP) qui dépasse les seuils configurés, afin d'empêcher toute nouvelle tentative jusqu'à ce que vous supprimiez manuellement la désactivation de l'adresse IP. Des services distincts sont disponibles pour les types d'attaques suivants :

- Tentatives d'authentification répétées et infructueuses vers les services VPN d'accès à

distance (attaques par analyse en force du nom d'utilisateur/mot de passe).
- Attaques d'initiation du client, où l'attaquant démarre mais ne termine pas les tentatives de connexion à une tête de réseau VPN d'accès à distance à plusieurs reprises à partir d'un hôte unique.
- La connexion tente d'accéder à des services VPN d'accès à distance non valides. C'est-à-dire, lorsque les pirates tentent de se connecter à des groupes de tunnels intégrés spécifiques destinés uniquement au fonctionnement interne du périphérique. Les terminaux légitimes ne peuvent jamais tenter de se connecter à ces groupes de tunnels.

Ces attaques, même si elles échouent dans leur tentative d'accès, peuvent consommer des ressources de calcul et empêcher les utilisateurs valides de se connecter aux services VPN d'accès à distance.

Lorsque vous activez ces services, le pare-feu de sécurité ferme automatiquement l'hôte (adresse IP) qui dépasse les seuils configurés, pour empêcher toute nouvelle tentative jusqu'à ce que vous supprimiez manuellement le shun de l'adresse IP.

 Remarque : tous les services de détection des menaces pour le VPN d'accès à distance sont désactivés par défaut.

Configurer

Connectez-vous à l'interface de ligne de commande (CLI) du pare-feu sécurisé en mode de configuration globale et activez un ou plusieurs des services de détection des menaces disponibles pour le VPN d'accès à distance :

Détection des menaces pour les tentatives de connexion à des services VPN internes uniquement (non valides)

Pour activer ce service, exécutez la commande threat-detection service invalid-vpn-access.

Détection des menaces pour les attaques d'initiation du client VPN d'accès distant

Pour activer ce service, exécutez la commande threat-detection service remote-access-client-

initiations hold-down <minutes> threshold <count>, où :

- hold-down <minutes> définit la période après la dernière tentative de démarrage pendant laquelle les tentatives de connexion consécutives sont comptées. Si le nombre de tentatives de connexion consécutives atteint le seuil configuré au cours de cette période, l'adresse IPv4 du pirate est ignorée. Vous pouvez définir cette période entre 1 et 1 440 minutes.

- threshold <count> est le nombre de tentatives de connexion nécessaires au cours de la période de retenue pour déclencher un shun. Vous pouvez définir le seuil entre 5 et 100.

Par exemple, si la période de retenue est de 10 minutes et que le seuil est de 20, l'adresse IPv4 est automatiquement désactivée en cas de 20 tentatives de connexion consécutives dans un délai de 10 minutes.

 Remarque : Lorsque vous définissez les valeurs de retenue et de seuil, tenez compte de l'utilisation de la NAT. Si vous utilisez la fonction PAT, qui autorise de nombreuses requêtes à partir de la même adresse IP, envisagez des valeurs plus élevées. Cela garantit que les utilisateurs valides disposent de suffisamment de temps pour se connecter. Par exemple, dans un hôtel, de nombreux utilisateurs peuvent tenter de se connecter en peu de temps.

Détection des menaces pour les échecs d'authentification VPN d'accès à distance

Pour activer ce service, exécutez la commande threat-detection service remote-access-authentication hold-down<minutes> threshold <count>, où :

- hold-down <minutes> définit la période après la dernière tentative infructueuse pendant laquelle les échecs consécutifs sont comptés. Si le nombre d'échecs d'authentification consécutifs atteint le seuil configuré au cours de cette période, l'adresse IPv4 du pirate est ignorée. Vous pouvez définir cette période entre 1 et 1 440 minutes.

- threshold <count> est le nombre de tentatives d'authentification ayant échoué, nécessaires au cours de la période de retenue pour déclencher un shun. Vous pouvez définir le seuil entre 1 et 100.

Par exemple, si la période de retenue est de 10 minutes et que le seuil est de 20, l'adresse IPv4 est automatiquement désactivée en cas de 20 échecs d'authentification consécutifs au cours d'une période de 10 minutes.

Remarque : Lorsque vous définissez les valeurs de retenue et de seuil, tenez compte de l'utilisation de la NAT. Si vous utilisez la fonction PAT, qui autorise de nombreuses requêtes à partir de la même adresse IP, envisagez des valeurs plus élevées. Cela garantit que les utilisateurs valides disposent de suffisamment de temps pour se connecter. Par exemple, dans un hôtel, de nombreux utilisateurs peuvent tenter de se connecter en peu de temps.

Remarque : Les échecs d'authentification via SAML ne sont pas encore pris en charge.

L'exemple de configuration suivant active les trois services de détection des menaces disponibles pour le VPN d'accès à distance avec une période de retenue de 10 minutes et un seuil de 20 pour l'initiation du client et les tentatives d'authentification ayant échoué.

```
threat-detection service invalid-vpn-access
threat-detection service remote-access-client-initiations hold-down 10 threshold 20
threat-detection service remote-access-authentication hold-down 10 threshold 20
```

Vérifier

Pour afficher les statistiques des services RAVPN de détection des menaces, exécutez la commande show threat-détection service [service] [entries|details]. Lorsque le service peut être : remote-access-authentication, remote-access-client-initiations ou invalid-vpn-access.

Vous pouvez limiter davantage la vue en ajoutant les paramètres suivants :

- entries : affiche uniquement les entrées suivies par le service de détection des menaces. Par exemple, les adresses IP dont les tentatives d'authentification ont échoué.
- details : affiche les détails et les entrées de service.

Exécutez la commande show threat-detection service pour afficher les statistiques de tous les services de détection de menaces qui sont activés.

```
ciscoasa# show threat-detection service
Service: invalid-vpn-access
    State     : Enabled
    Hold-down : 1 minutes
    Threshold : 1
    Stats:
        failed      :          0
        blocking    :          0
        recording   :          0
        unsupported :          0
        disabled    :          0
    Total entries: 0
Service: remote-access-authentication
    State     : Enabled
    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
        blocking    :          1
        recording   :          4
        unsupported :          0
        disabled    :          0
    Total entries: 2
Name: remote-access-client-initiations
    State     : Enabled
    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
        blocking    :          0
        recording   :          0
        unsupported :          0
        disabled    :          0
    Total entries: 0
```

Pour afficher plus de détails sur les agresseurs potentiels qui sont suivis pour le service d'authentification d'accès à distance, exécutez la commande show threat-detection service <service>entries.

```
ciscoasa# show threat-detection service remote-access-authentication entries
Service: remote-access-authentication
    Total entries: 2

Idx Source              Interface            Count          Age        Hold-down
--- ------------------- -------------------- -------------- ---------- ---------
  1 192.168.100.101/ 32              outside              1        721         0
  2 192.168.100.102/ 32              outside              2        486       114
Total number of IPv4 entries: 2

NOTE: Age is in seconds since last reported. Hold-down is in seconds remaining.
```

Pour afficher les statistiques générales et les détails d'un service VPN d'accès à distance de détection des menaces spécifique, exécutez la commande show threat-détection service <service> details.

```
ciscoasa# show threat-detection service remote-access-authentication details
Service: remote-access-authentication
    State     : Enabled
    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
        blocking    :          1
        recording   :          4
        unsupported :          0
        disabled    :          0
     Total entries: 2

Idx Source              Interface            Count          Age         Hold-down
--- ------------------- -------------------- -------------- ----------- ---------
  1 192.168.100.101/ 32              outside              1         721          0
  2 192.168.100.102/ 32              outside              2         486        114
Total number of IPv4 entries: 2

NOTE: Age is in seconds since last reported. Hold-down is in seconds remaining.
```

Remarque : Les entrées affichent uniquement les adresses IP suivies par le service de détection des menaces. Si une adresse IP remplit les conditions pour être désactivée, le nombre de blocages augmente et l'adresse IP n'est plus affichée comme entrée.

En outre, vous pouvez surveiller les shuns appliqués par les services VPN, et supprimer les shuns pour une adresse IP unique ou toutes les adresses IP avec les commandes suivantes :

- show shun [adresse_ip]

Affiche les hôtes désactivés, y compris ceux qui sont automatiquement désactivés par la détection des menaces pour les services VPN, ou manuellement à l'aide de la commande shun. Vous pouvez éventuellement limiter l'affichage à une adresse IP spécifiée.

- no shun ip_address [interface if_name]

Supprime un shun appliqué à l'adresse IP spécifiée.

Si une adresse IP est désactivée sur plusieurs interfaces et qu'aucune interface spécifique n'est mentionnée, la commande supprime la désactivation d'une seule interface. La sélection de cette interface est basée sur une recherche de route pour l'adresse IP shuntée. Pour supprimer le shun des interfaces supplémentaires, vous devez spécifier explicitement l'interface.

- clear shun

Supprime le shun de toutes les adresses IP et interfaces.

Remarque : Les adresses IP rejetées par la détection de menaces pour les services VPN n'apparaissent pas dans la commande show threat-detection shun, qui s'applique uniquement à la détection de menaces d'analyse.

Pour lire tous les détails de chaque sortie de commande et les messages syslog disponibles relatifs aux services de détection des menaces pour VPN d'accès à distance, veuillez vous reporter au Guide de configuration CLI du pare-feu ASA Cisco Secure Firewall, 9.20. Chapitre : Document Threat Detection.

Informations connexes

- Pour obtenir de l'aide supplémentaire, contactez le centre d'assistance technique (TAC). Un contrat d'assistance valide est requis : Contacts d'assistance internationale Cisco.
- Vous pouvez également visiter la communauté VPN Cisco ici.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.