Configurer l'accès aux ressources internes pour les utilisateurs VPN sur FTD avec trafic HairPin

Table des matières

Problème

L'objectif est d'activer l'accès complet des utilisateurs VPN aux ressources réseau internes après une authentification VPN réussie à l'aide de RADIUS (sur un serveur joint à un domaine Windows) sur Cisco Secure Firewall FTD.

La configuration VPN est déjà opérationnelle ; les utilisateurs peuvent télécharger et installer le client VPN et s'authentifier avec succès. Le problème se concentre sur la configuration du contrôle d'accès et des règles NAT nécessaires pour permettre l'accès aux ressources internes nécessaires sur le VPN.

Environnement

- Produit : Cisco Secure Firewall Firepower (FTD), version 7.6.0 (tel qu'un appareil CSF1220CX)
- Gestion : Firepower Management Center (FMC), FMC cloud (cdFMC) ou Firepower Device Manager (FDM)
- VPN : configuré avec l'authentification RADIUS sur un serveur Windows joint au domaine (NPS)
- Pool d'adresses VPN : 192.168.250.1 - 192.168.250.200
- Exemple de sous-réseau interne cible : 192.168.95.0/24
- Version du logiciel : 9.22.1 (comme indiqué dans le workflow)
- Interfaces pertinentes : interface « externe » pour l'entrée VPN
- Accès RDP et Active Directory requis sur une connexion VPN

Résolution

Ces étapes détaillent la configuration requise pour permettre aux utilisateurs VPN d'accéder aux ressources internes (telles que RDP et Active Directory) sur Cisco FTD. Cela inclut la création de règles de stratégie d'accès, la configuration des exemptions NAT et de la NAT hairpin pour le trafic VPN, et l'utilisation de commandes de dépannage pour valider la configuration.

Étape 1 : ajoutez une entrée de liste d'accès pour permettre au pool d'adresses VPN d'accéder aux ressources internes.

```
access-list CSM_FW_ACL_ advanced permit ip object VPN_Pool any rule-id 268438528
```

```
access-list CSM_FW_ACL_ remark rule-id 268438528: ACCESS POLICY: Default Access Control Policy - Mandat
access-list CSM_FW_ACL_ remark rule-id 268438528: L7 RULE: Permit_VPN_Pool
```

Étape 2 : ajoutez une règle de liste d'accès pour permettre aux ressources internes d'envoyer le trafic de retour au pool VPN :

```
access-list CSM_FW_ACL_ advanced permit ip any object VPN_Pool
```

Ces règles peuvent ensuite être renforcées pour restreindre des sources et des destinations spécifiques, le cas échéant.

Étape 3 : Configurez l'exemption NAT ou la NAT en épingle à cheveux pour le trafic VPN

Il existe deux approches communes :

- ◦ Option A : exemption NAT pour le pool VPN vers le sous-réseau interne

```
nat (outside,inside) source static VPN_Pool VPN_Pool destination static Net_192.168.95.1-24 Net_192.168
```

- ◦ Option B : NAT en épingle à cheveux pour pool VPN sur la même interface (no-proxy-arp)

```
nat (any,any) source static VPN_Pool VPN_Pool no-proxy-arp
```

- ◦ Option C : NAT en épingle à cheveux dynamique pour pool VPN sur interface externe

```
nat (outside,outside) dynamic VPN_Pool interface
```

La méthode correcte dépend du fait que les ressources internes se trouvent sur la même interface physique (nécessitant la NAT hairpin) ou sur des interfaces différentes (exemption NAT).

Étape 4 : utilisez la commande `packet-tracer` pour simuler les flux de trafic du pool VPN vers les ressources internes et valider si le trafic est autorisé par la règle, la NAT et la route prévues.

```
packet-tracer input outside icmp 192.168.250.1 8 0 192.168.95.1
packet-tracer input outside tcp 192.168.250.1 12345 192.168.95.1 80
packet-tracer input inside icmp 192.168.95.1 8 0 192.168.250.1
```

```
packet-tracer input inside tcp 192.168.250.1 54321 192.168.95.1 443
--
Phase 5
ID: 5
Type: ACCESS-LIST
Result: ALLOW
Config: access-group CSM_FW_ACL_ globalaccess-list CSM_FW_ACL_ advanced permit ip object VPN_Pool any r
Additional Information:  This packet will be sent to snort for additional processing where a verdict wi
Elapsed Time: 0 ns
--
Phase 7
ID: 7
Type: NAT
Result: ALLOW
Config: nat (outside,outside) dynamic VPN_Pool interface
Additional Information: Static translate 192.168.250.1/12345 to 192.168.250.1/12345 Forward Flow based
Elapsed Time: 0 ns
```

Remarque : la sortie du traceur de paquets pour la phase WebVPN peut afficher un « DROP » pour le trafic VPN sur l'interface externe. Ce comportement est attendu pour le trafic en texte clair sur l'interface externe et peut toujours être utilisé pour valider la NAT.

Notes supplémentaires:

- Il est possible que les captures de paquets dans l'interface de défense contre les menaces n'affichent que les demandes entrantes. Si aucune suppression n'est observée, mais que le trafic n'atteint pas la ressource interne, vérifiez les règles NAT et de liste d'accès.
- Lorsque SSH n'est pas disponible, tous les dépannages peuvent être effectués via les fonctions de l'interface utilisateur de Threat Defense dans cdFMC, mais l'utilisation des commandes est limitée.
- Il est possible que certaines modifications soient nécessaires sur des périphériques adjacents pour une connectivité de bout en bout.

Motif

La cause principale était une stratégie d'accès et une configuration NAT insuffisantes pour le trafic VPN vers interne et interne vers pool VPN. La configuration par défaut ne permettait pas une communication bidirectionnelle complète du pool VPN vers les ressources internes et inversement, ni ne gérait les exigences NAT en épingle à cheveux pour l'entrée et la sortie du trafic sur la même interface.

Autres informations utiles

- Configurer l'exemption NAT sur FTD
- Assistance technique de Cisco et téléchargements

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.