Foire aux questions

Foire aux questions

Q. Quelles sont les nouvelles fonctionnalités prises en charge par la version 4.0 de l'outil de migration Secure Firewall ?

A. Les fonctionnalités suivantes sont prises en charge avec la version 4.0 :

- Migration d'un appareil géré par FDM vers un appareil de défense contre les menaces géré par le centre de gestion ou le centre de gestion de pare-feu fourni dans le nuage.
- Migration des routes ECMP (Equal Cost Multi-Path) à partir d'ASA.
- Migration du routage basé sur les politiques (PBR) à partir d'ASA.
- Migration des attributs personnalisés du VPN d'accès à distance et de l'équilibrage de charge du VPN à partir d'ASA.

Q. Quelles sont les nouvelles fonctionnalités prises en charge par l'outil de migration Secure Firewall version 3.0.1?

A. Les caractéristiques suivantes sont prises en charge avec la version 3.0.1 :

- Migration du protocole EIGRP (Enhanced Interior Gateway Routing Protocol) depuis l'ASA.
- La gamme Secure Firewall 3100 est prise en charge en tant que périphérique source ou de destination pour les migrations ASA.

Q. Quelles sont les nouvelles fonctionnalités prises en charge par la version 3.0 de l'outil de migration Secure Firewall?

A. Les caractéristiques suivantes sont prises en charge avec la version 3.0 :

- Migration du VPN d'accès à distance
- Migration vers le centre de gestion de pare-feu en nuage

Q. Quelles sont les nouvelles fonctionnalités prises en charge par la version 2.5.1 de l'outil de migration Secure Firewall?

A. Les caractéristiques suivantes sont prises en charge avec la version 2.5.1 :

- Objets de routage dynamique
- Protocole de passerelle frontière

Q. Quelles sont les nouvelles fonctionnalités prises en charge par la version 2.5 de l'outil de migration Secure Firewall?

A. Les fonctionnalités suivantes sont prises en charge avec la version 2.5 :

- Optimisation ACL
- Masque générique

Q. Quelles sont les nouvelles fonctionnalités prises en charge par la version 2.4 de l'outil de migration Secure Firewall ?

A. Migration de la configuration VPN ASA suivante vers la protection contre les menaces :

- VPN basé sur une carte cryptographique (statique/dynamique) à partir de l'ASA
- VPN ASA basé sur les routes (VTI)
- Migration vers un VPN basé sur des certificats à partir d'ASA

Q. Quelles sont les nouvelles fonctionnalités prises en charge par l'outil de migration Secure Firewall version 2.3.5 ?

A. Les fonctionnalités suivantes sont prises en charge avec la version 2.3.5 :

- Interface de tunnel virtuel (VTI) et configurations connexes dans les routes statiques, ACL.
- Tunnels VPN basés sur le routage (VTI)

Q. Quelles sont les nouvelles fonctionnalités prises en charge par la version 2.3.4 de l'outil de migration Secure Firewall?

A. Les fonctionnalités suivantes sont prises en charge avec la version 2.3.4 :

- Objets VPN
- Tunnels de réseau privé virtuel (VPN) de site à site

Q. Quelles sont les plateformes source et cible que l'outil de migration Secure Firewall peut faire migrer?

A. L'outil de migration Secure Firewall peut migrer les politiques de la plateforme ASA prise en charge vers la plateforme de défense contre les menaces. Pour en savoir plus, consultez Plateformes ASA source prises en charge.

Q. Quelles sont les tâches que vous devez effectuer dans les rapports de prémigration et de postmigration?

A. Pour effectuer les tâches dans le cadre de votre plan de migration d'ASA vers Firewall Threat Defense, consultez la section Exemple de migration : ASA vers Threat Defense 2100.

Q. Quelles sont les versions des plateformes de destination prises en charge?

A. Vous pouvez utiliser l'outil de migration Secure Firewall pour migrer une configuration ASA vers l'instance autonome ou de conteneur des plateformes de pare-feu Threat Defense pour le centre de gestion

6.2.3 ou une version ultérieure. Pour plus d'informations sur la liste des périphériques pris en charge, consultez.Plateformes Défense contre les menaces cibles prises en charge

Q. Quelles sont les fonctionnalités prises en charge par l'outil de migration Secure Firewall pour la migration?

A. L'outil de migration Secure Firewall prend en charge la migration de la configuration L3/L4 ASA vers la protection contre les menaces. Il permet également d'activer des fonctionnalités L7 comme IPS, la politique de fichiers, etc., pendant le processus de migration.

L'outil de migration Secure Firewall peut migrer entièrement les configurations ASA suivantes :

- Objets et groupes réseau (sauf les masques non contigus)
- Objets de service, à l'exception des objets de service configurés pour une source et une destination

Remarque Bien que l'outil de migration de pare-feu sécurisé ne migre pas les objets de service élargis (configurés pour une source et une destination), les règles ACL et NAT référencées sont migrées avec toutes leurs fonctionnalités.

- Groupes d'objets de service, à l'exception des groupes d'objets de service imbriqués, des objets VPN et de la migration VPN cryptographique ASA

Remarque Puisque l'imbrication n'est pas prise en charge sur le centre de gestion, l'outil de migration Cisco Secure Firewall élargit le contenu des règles référencées. Les règles sont toutefois migrées avec toutes les fonctionnalités.

- Objets et groupes FQDN IPv4 et IPv6
- Prise en charge de la conversion IPv6 (interface, routes statiques, objets, ACL et NAT)
- Règles d'accès appliquées aux interfaces dans la direction entrante et ACL globales
- NAT automatique, NAT manuel et NAT d'objet (conditionnel)
- Routes statiques, à l'exception de celles configurées avec l'option de suivi qui sont partiellement migrées et des routes ECMP qui ne sont pas migrées
- Interfaces physiques
- Sous-interfaces
- canaux de port
- Groupes de ponts (mode transparent uniquement)
- Règles de politique de contrôle d'accès basées sur le protocole de tunnellisation (migrées en tant que règles de tunnel de préfiltre)
- Règle basée sur les catégories pour les configurations gérées par CSM
- IP SLA Monitor
- Recherche groupée d'objets
- Objets temporels

- Objets VPN
- Interfaces VTI
- Tunnels VPN basés sur des politiques (Crypto Map) et basés sur le routage (VTI)
- Migration VPN basée sur des certificats d'ASA vers la protection contre les menaces
- Objets de routage dynamique pour EIGRP et BGP
- VPN d'accès à distance

Q. Quelles sont les nouvelles fonctionnalités prises en charge par l'outil de migration Secure Firewall pour la version 2.2 ?

A. Les fonctionnalités suivantes sont prises en charge avec la version 2.2 :

- Recherche groupée d'objets
- IP SLA Monitor
- Objets temporels

Q. Quelles sont les nouvelles fonctionnalités prises en charge par l'outil de migration Secure Firewall pour la version 2.0 ?

A. Les fonctionnalités suivantes sont prises en charge avec la version 2.0 :

- Mappage de la zone de destination pour les règles d'accès
- Règles de tunnel préfiltrées
- Règles basées sur les catégories
- Limite de politique et avertissement de capacité
- Prise en charge de la migration ASA 5505 et ASA-SM

Q. Y a-t-il une dépendance au centre de gestion pour utiliser les nouvelles fonctionnalités introduites dans l'outil de migration Secure Firewall?

A. Oui. Les fonctionnalités suivantes sont prises en charge avec le centre de gestion cible 6.5 et les versions ultérieures :

- Faire migrer les règles de tunnel en tant que préfiltre
- Règles basées sur les catégories
- Migration d'ASA 5505

Remarque Nécessite la version 6.5 ou ultérieure du centre de gestion pour migrer vers la plateforme de défense contre les menaces FPR-1010.

Les fonctionnalités suivantes sont prises en charge avec le centre de gestion cible 6.6 et les versions ultérieures :

- Recherche groupée d'objets

- IP SLA Monitor
- Objets temporels
- Objets VPN
- Tunnels de réseau privé virtuel (VPN) de site à site

Les fonctionnalités suivantes sont prises en charge avec le centre de gestion cible 6.7 et les versions ultérieures :

- Interface VTI et routes statiques associées.
- Configuration VPN de type d'authentification de clé pré-partagée basée sur le routage (VTI) vers le centre de gestion.
- Créez une zone de sécurité routée, ajoutez des interfaces VTI, puis définissez des règles de contrôle d'accès pour le contrôle du trafic décrypté sur le tunnel VTI.

Les fonctionnalités suivantes sont prises en charge avec le centre de gestion cible 7.1 et les versions ultérieures :

- Objets de routage dynamique
- BGP

Les fonctionnalités suivantes sont prises en charge avec le centre de gestion cible 7.2 et les versions ultérieures :

- VPN d'accès à distance
- EIGRP

Q. Pouvons-nous migrer toutes les règles d'accès de la configuration source vers la politique de préfiltre ?

A. Non. Pour les migrations choisies avec les **règles de tunnel de migration comme préfiltre**, l'outil de migration Secure Firewall identifie les règles d'accès basées sur le protocole de tunnellisation et les fait migrer en tant que règles de tunnel.

Q. Quelles sont les fonctionnalités que l'outil de migration Secure Firewall ne migre pas aujourd'hui?

A. L'outil de migration Secure Firewall ne prend pas en charge les configurations ASA suivantes pour la migration. Si ces configurations sont prises en charge dans le centre de gestion, vous pouvez les configurer manuellement une fois la migration terminée.

- Règles de politique de contrôle d'accès basées sur SGT
- Objets basés sur SGT
- Règles de politique de contrôle d'accès basées sur l'utilisateur
- Règles NAT configurées avec l'option d'allocation de bloc
- Objets avec un type et un code ICMP non pris en charge
- Règles de contrôle d'accès basées sur le protocole de tunnellisation
- Règles NAT configurées avec SCTP
- Règles NAT configurées avec l'hôte « 0.0.0.0 »

- Règles de politique de contrôle d'accès basées sur le protocole de tunnellisation (prise en charge à partir de l'outil de migration Secure Firewall 2.0 avec le centre de gestion cible 6.5 et versions ultérieures)
- Carte de chiffrement dynamique basée sur le VPN
- Configuration VPN basée sur l'authentification des certificats

Pour en savoir plus, consultez Lignes directrices et limites relatives à la licence.

Q. Quels sont les périphériques sources et la version du code pris en charge?

A. Vous pouvez utiliser l'outil de migration Secure Firewall pour faire migrer la configuration à partir de plateformes ASA à contexte unique ou à contexte multiple (version logiciel 8.4 ou plus récent) Pour plus d'informations sur la liste des périphériques, consultez Plateformes ASA source prises en charge.

Q. L'outil de migration Secure Firewall prend-il en charge la migration d'ASA à contextes multiples?

A. Oui. L'outil de migration Secure Firewall peut gérer la migration d'ASA à contextes multiples. À tout moment, il est possible de faire migrer un contexte de l'ASA (à l'exception du contexte *système*) vers un conteneur de défense contre les menaces ou des instances natives du centre de gestion cible.

Q. Quel est le mécanisme d'assistance en cas d'erreurs de migration?

A. L'outil de migration Secure Firewall est intégré à Cisco Success Network. En cas d'erreurs ou de problèmes, communiquez avec le TAC de Cisco. Pour le dépannage, consultez Dépannage des problèmes de migration.

Q. Combien de temps faut-il à l'outil de migration Secure Firewall pour réussir la migration d'une configuration?

A. Le temps nécessaire à la migration dépend de nombreux facteurs tels que la latence du réseau, la charge du centre de gestion, la taille de la configuration, le nombre d'objets, la liste de contrôle d'accès, etc. Lors de tests internes, il a été observé qu'un fichier de configuration de 2,0 Mo avec plus de 7 000 listes de contrôle d'accès, plus de 7 000 traductions NAT et plus de 3 000 objets réseau prend environ 6 minutes pour terminer la migration.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.