La configuration NAT et les recommandations ASA pour Expressway-e conjuguent implémentation d'interfaces réseau.

Contenu

Introduction

Ce document décrit comment implémenter la configuration de Traduction d'adresses de réseau (NAT) exigée dans l'appliance de sécurité adaptable Cisco (ASA) pour Expressway-e et interfaces réseau d'Expressway-C de doubles/double implémentation du contrôleur d'interface réseau (NIC).

Ce déploiement est l'option recommandée pour des déploiements des périphériques d'Expressway-e et d'Expressway-C (plutôt que le Simple-NIC avec la réflexion NAT).

Contribué par le chrétien G. Hernandez R. et Cesar Lopez Zamarripa, ingénieurs TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration de base de Cisco ASA et configuration NAT
- Configuration de base de Cisco Expressway-e et d'Expressway-C

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco ASA 5500 et appliances de gamme 5500-X qui exécutent la version de logiciel 8.0 et plus tard.
- Version X8.0 de Cisco Expressway et plus tard.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle commande.

> **Note**: Par le document entier, des périphériques d'Expressway sont référés comme Expressway-e et Expressway-C. Cependant, la même configuration applique au serveur de communication vidéo (VCS) Expressway et des périphériques de contrôle de VCS.

Informations générales

Par conception, Cisco Expressway-e peut être placé dans une zone démilitarisée (DMZ) ou avec une interface d'Internet-revêtement, alors qu'il peut communiquer avec Cisco Expressway-C dans un réseau privé. Quand Cisco Expressway-e est placé dans un DMZ, ce sont les allocations complémentaires :

- Dans le scénario le plus commun, Cisco Expressway-e est géré du réseau privé. Quand Cisco Expressway-e est dans un DMZ, un Pare-feu (externe) de périmètre peut être utilisé pour bloquer l'accès non désiré à Expressway des réseaux externes par l'intermédiaire de l'hypertexte Transfer Protocol des demandes sécurisées (HTTPS) ou de Protocole Secure Shell (SSH).

- Si le DMZ ne permet pas les liaisons directes entre interne et les réseaux externes, des serveurs dédiés sont exigés pour traiter le trafic qui traverse le DMZ. Cisco Expressway peut agir en tant que serveur proxy pour le Protocole SIP (Session Initiation Protocol) et/ou H.323 exprimer et le trafic visuel. Dans ce cas, vous pouvez utiliser la double option d'interfaces réseau qui permet à Cisco Expressway pour avoir deux adresses IP différentes, une pour le trafic à/de le pare-feu externe, et une pour le trafic à/de le Pare-feu interne.

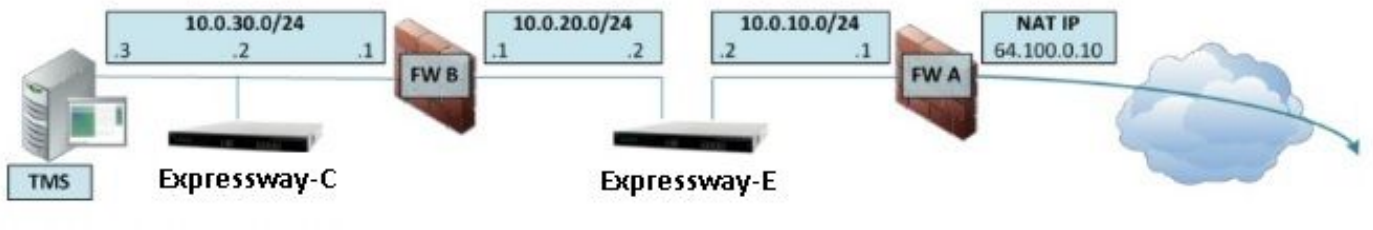
- Cette installation empêche les liaisons directes du réseau externe au réseau interne. Ceci

améliore la combinaison de Sécurité de réseau interne.

Conseil : Afin d'obtenir plus de détails au sujet de l'implémentation de TelePresence, référez-vous à Cisco Expressway-e et à Expressway-C - guide de déploiement de configuration de base et placement d'un VCS Expressway de Cisco dans un DMZ plutôt que dans l'Internet public.

C d'Expressway et E - Doubles interfaces réseau/double implémentation NIC

Cette image affiche un déploiement d'exemple pour Expressway-e avec de doubles interfaces réseau et NAT statique. Expressway-C agit en tant que client de traversée. Il y a deux Pare-feu (FW A et FWB). Typiquement, dans cette configuration DMZ, FW A ne peut pas conduire le trafic à FW B, et des périphériques tels qu'Expressway-e sont exigés pour valider et expédier le trafic du sous-réseau FW A au sous-réseau FW b (et vice versa).



Ce déploiement se compose de ces composants.

Sous-réseau DMZ 1 – 10.0.10.0/24

- Interface interne FW A – 10.0.10.1
- Interface d'Expressway-e LAN2 – 10.0.10.2

Sous-réseau DMZ 2 – 10.0.20.0/24

- Interface externe FW B – 10.0.20.1
- Interface d'Expressway-e LAN1 – 10.0.20.2

Sous-réseau LAN – 10.0.30.0/24

- Interface interne FW B – 10.0.30.1
- Interface d'Expressway-C LAN1 – 10.0.30.2
- Interface de réseau serveur de la suite logicielle de gestion Cisco TelePresence (TMS) – 10.0.30.3

Particularités de cette implémentation :

- FW A est le Pare-feu externe ou de périmètre ; il est configuré avec IP NAT (IP de public) de 64.100.0.10 qui est statiquement traduit à 10.0.10.2 (l'interface d'Expressway-e LAN2)
- FW B est le Pare-feu interne
- Expressway-e LAN1 a le mode NAT statique désactivé
- Expressway-e LAN2 a le mode NAT statique activé avec l'adresse NAT statique 64.100.0.10
- Expressway-C a une zone de client de traversée qui indique 10.0.20.2 (l'interface d'Expressway-e LAN1)
- Il n'y a aucun routage entre 10.0.20.0/24 et 10.0.10.0/24 sous-réseaux. Expressway-e jette un pont sur ces sous-réseaux et agit en tant que support de proxy pour la signalisation SIP/H.323

et le Protocole RTP (Real-Time Transport Protocol)/Control Protocol de RTP (RTCP).
- Cisco TMS a Expressway-e configuré avec l'adresse IP 10.0.20.2

Conditions requises/limites

Sous-réseaux non-recouverts

Si Expressway-e est configuré pour utiliser les deux interfaces de RÉSEAU LOCAL, la nécessité des interfaces LAN1 et LAN2 se trouvent dans des sous-réseaux non-recouverts pour s'assurer que le trafic est envoyé à l'interface appropriée.

Groupement

En groupant des périphériques d'Expressway avec l'option **avancée de réseau** configurée, chaque pair de batterie doit être configuré avec sa propre adresse de l'interface LAN1. En outre, le groupement doit être configuré sur une interface qui n'a pas le mode NAT statique activé. Par conséquent, il est recommandé que vous utilisez le LAN2 comme interface externe, sur laquelle vous pouvez appliquer et configurer NAT statique le cas échéant.

Paramètres d'interface externes de RÉSEAU LOCAL

Les configurations externes de configuration d'interface de RÉSEAU LOCAL sur le contrôle de page de configuration IP que l'interface réseau utilise transversal utilisant des relais autour de NAT (TOUR). Dans une configuration d'Expressway-e de double interface réseau, ceci est normalement placé à l'interface externe de RÉSEAU LOCAL d'Expressway-e.

Routes statique

Expressway-e doit être configuré avec une adresse de passerelle par défaut de 10.0.10.1 pour ce scénario. Ceci signifie que tout le trafic envoyé par l'intermédiaire du LAN2, par défaut, est envoyé à l'adresse IP 10.0.10.1.

Si FW B traduit le trafic envoyé du sous-réseau 10.0.30.0/24 à l'interface d'Expressway-e LAN1 (par exemple, le trafic de client de traversée d'Expressway-C ou le trafic d'administration de serveurs TMS), ce trafic apparaît pendant qu'il provient l'interface externe FWB (10.0.20.1) comme elle atteint Expressway-e LAN1. Expressway-e peut alors répondre à ce trafic par l'intermédiaire de son interface LAN1 puisque la source apparente de ce trafic se trouve sur le même sous-réseau.

Si NAT est activé sur FW B, le trafic envoyé d'Expressway-C à Expressway-e LAN1 affiche pendant qu'il provient 10.0.30.2. Si Expressway n'a pas une artère statique ajoutée pour le sous-réseau 10.0.30.0/24, il envoie les réponses pour ce trafic à sa passerelle par défaut (10.0.10.1) du LAN2, car il ne se rend pas compte que le sous-réseau 10.0.30.0/24 se trouve derrière le Pare-feu interne (FW B). Par conséquent, une artère statique doit être ajoutée, exécutent la commande de **RouteAdd** CLI de **xCommand** par une session de SSH à Expressway.

Dans cet exemple particulier, Expressway-e doit savoir qu'il peut atteindre le sous-réseau 10.0.30.0/24 derrière FW B, qui est accessible par l'intermédiaire de l'interface LAN1. Pour accomplir ceci, exécutez la commande :

```
xCommand RouteAdd Address: 10.0.30.0 PrefixLength: 24 Gateway: 10.0.20.1 Interface: LAN1
```

> **Note**: La configuration de route statique peut être appliquée par le **système de l'**interface utilisateur graphique (GUI) aussi bien que de la section d'Expressway-e**/réseau > interfaces/artères de charge statique**. ########

Dans cet exemple, le paramètre d'interface peut également être placé à l'**automatique** car l'adresse de passerelle (10.0.20.1) est seulement accessible par l'intermédiaire du LAN1.

Si NAT n'est pas activé sur FW B et besoins d'Expressway-e de communiquer avec des périphériques dans les sous-réseaux (autre que 10.0.30.0/24) qui sont également situés derrière FW B, les artères statiques doit être ajouté pour ces périphériques/sous-réseaux.

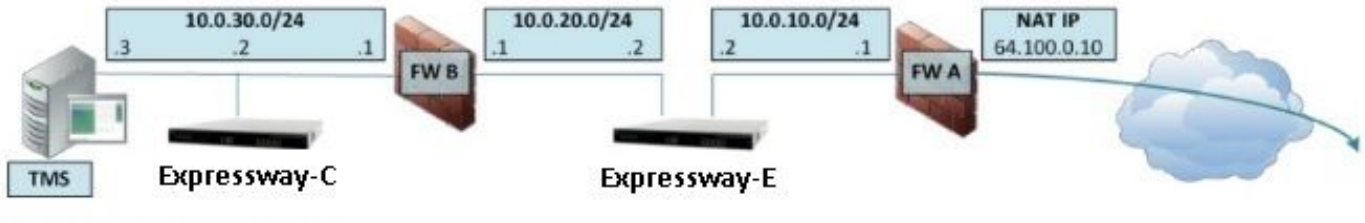
> **Note**: Ceci inclut des connexions de SSH et HTTPS des postes de travail de Gestion de réseau ou pour des services réseau comme le NTP, les DN, le LDAP/AD, ou le Syslog.

La commande et la syntaxe de **RouteAdd de xCommand** sont décrites dans le détail complet dans le *guide de l'administrateur de VCS.*

Configuration

Cette section décrit comment configurer le NAT statique exigé pour de doubles interfaces réseau d'Expressway-C et d'Expressway-e/double implémentation NIC sur l'ASA. Quelques recommandations modulaires supplémentaires de configuration du cadre de stratégie ASA (MPF) sont incluses pour traiter le trafic SIP/H323.

C d'Expressway et E - Doubles interfaces réseau/double implémentation NIC



Dans cet exemple, l'affectation d'adresse IP sont la prochaine.

IP address:10.0.30.2/24 d'Expressway-C

Passerelle par défaut d'Expressway-C : 10.0.30.1 (FW-B)

Adresses IP d'Expressway-e

Sur le LAN2 : 10.0.10.2/24

Sur le LAN1 : 10.0.20.2/24

Passerelle par défaut d'Expressway-e : 10.0.10.1 (FW-A)

Adresse IP TMS : 10.0.30.3/24

Configuration FW-A :

Étape 1. Configuration NAT statique pour Expressway-e

Comme expliqué dans la **section Informations générales de** ce document, le FW-A a une traduction NAT statique pour permettre à Expressway-e pour être accessible de l'Internet utilisant l'adresse IP publique 64.100.0.10. Est NATed à l'adresse IP 10.0.10.2/24 d'Expressway-e LAN2. Qu'étant dit, c'est la configuration NAT statique exigée FW-A.

Pour des versions 8.3 et ultérieures ASA :

```
! To use PAT with specific ports range:

object network obj-10.0.10.2
host 10.0.10.2

object service obj-udp_3478-3483 service udp source range 3478 3483 object service obj-
udp_24000-29999 service udp source range 24000 29999 object service obj-udp_36002-59999 service
udp source range 36002 59999 object service obj-tcp_5222 service tcp source eq 5222 object
service obj-tcp_8443 service tcp source eq 8443 object service obj-tcp_5061 service tcp source
eq 5061 object service obj-udp_5061 service udp source eq 5061 nat (inside,outside) source
static obj-10.0.10.2 interface service obj-udp_3478-3483 obj-udp_3478-3483 nat (inside,outside)
source static obj-10.0.10.2 interface service obj-udp_24000-29999 obj-udp_24000-29999 nat
(inside,outside) source static obj-10.0.10.2 interface service obj-udp_36002-59999 obj-
udp_36002-59999 nat (inside,outside) source static obj-10.0.10.2 interface service obj-tcp_5222
obj-tcp_5222 nat (inside,outside) source static obj-10.0.10.2 interface service obj-tcp_8443
obj-tcp_8443 nat (inside,outside) source static obj-10.0.10.2 interface service obj-tcp_5061
obj-tcp_5061 nat (inside,outside) source static obj-10.0.10.2 interface service obj-udp_5061
obj-udp_5061 OR

! To use with static one-to-one NAT:

object network obj-10.0.10.2
nat (inside,outside) static interface
```

> **Note: En essayant d'appliquer le PAT statique vous commande reçoivent ce message d'erreur sur l'interface de ligne de commande ASA, « ERREUR : Incapable NAT de réserver des ports ». Puis clair les entrées de xlate avec les gens du pays x.x.x.x de clear xlate de commande où x.x.x.x correspond à l'ASA en dehors de l'adresse IP. Cette commande efface toutes les traductions associées avec cet IP, ainsi dans les environnements de production, l'exécutent avec prudence.**
> Le ### a besoin de clarification

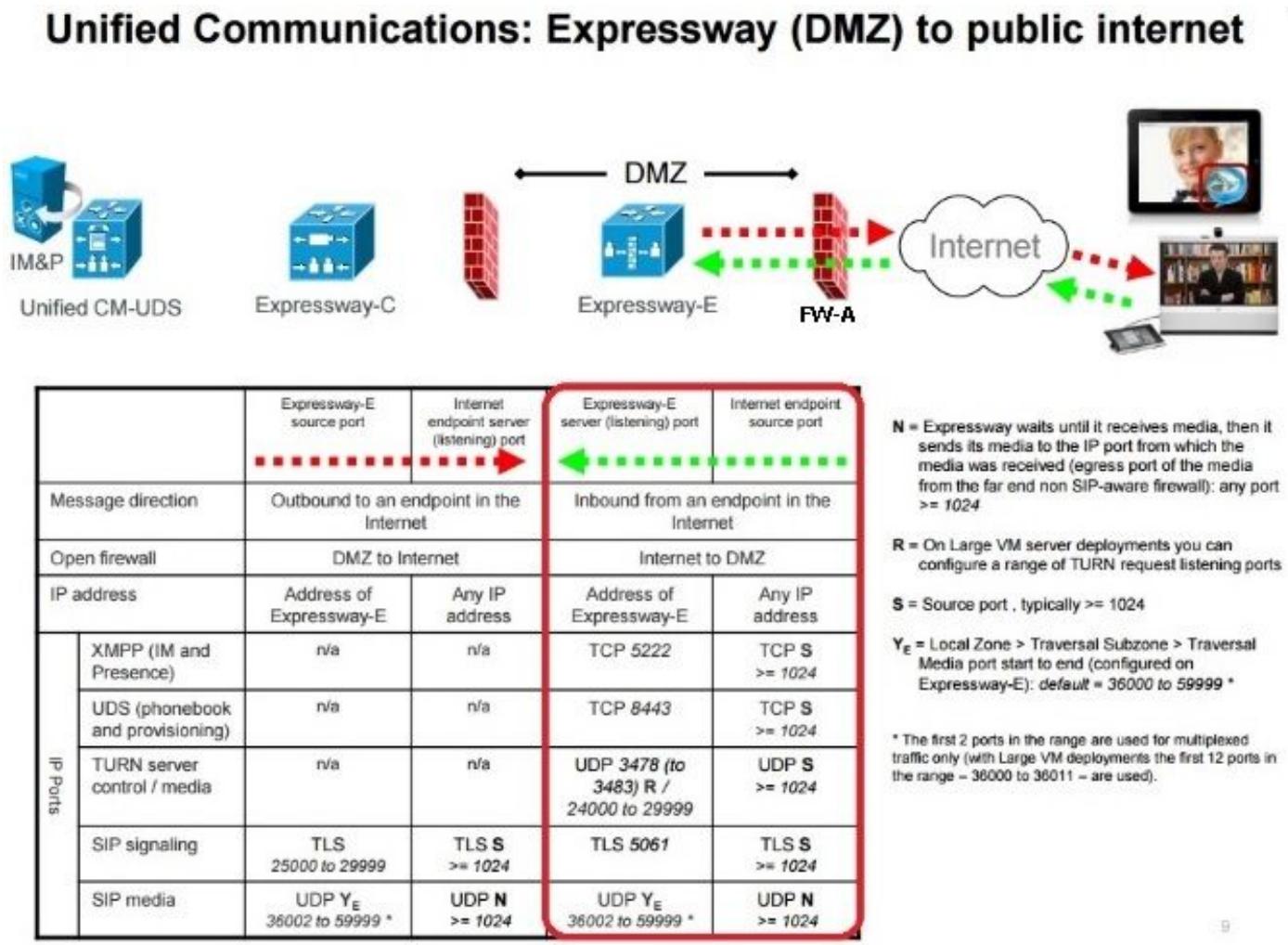
Pour des versions 8.2 et antérieures ASA :

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This example shows only when Static one-to-one NAT is used.

static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

Étape 2. Configuration de liste de contrôle d'accès (ACL) pour permettre les ports requis de l'Internet à Expressway-e

Selon la transmission unifiée : Expressway (DMZ) à la documentation d'Internet public, ceci est la liste de TCP et de ports UDP des lesquels Expressway-e exige pour être permis dans FW-A :



C'est la configuration d'ACL exigée comme d'arrivée dans le FW A en dehors de l'interface.

Pour des versions 8.3 et ultérieures ASA.

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This example shows only when Static one-to-one NAT is used.

static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

Pour des versions 8.2 et antérieures ASA.

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This example shows only when Static one-to-one NAT is used.

static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

> **Note**: Il est fortement recommandé pour désactiver le SIP et H.323 des inspections sur le trafic réseau de transport de Pare-feu à ou d'Expressway-e, comme une fois activées, ceci s'avère fréquemment pour affecter négativement la fonctionnalité intégrée de traversée d'Expressway-e firewall/NAT.

Configuration FW-B

Comme expliqué dans la **section Informations générales de** ce document, FW B peut exiger d'un NAT ou d'une configuration PAT dynamique de permettre le sous-réseau interne 10.0.30.0/24 à traduire à l'adresse IP 10.0.20.1 en sortant à l'interface extérieure du FW B.

Pour des versions 8.3 et ultérieures ASA :

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This example shows only when Static one-to-one NAT is used.

static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

Pour des versions 8.2 et antérieures ASA :

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This example shows only when Static one-to-one NAT is used.

static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

> **Note**: Il est fortement recommandé pour désactiver le SIP et H.323 les inspections sur le trafic réseau de transport de Pare-feu à ou d'Expressway-e, comme une fois activé ceci s'avère fréquemment affecter négativement la fonctionnalité intégrée de traversée d'Expressway-e firewall/NAT.

> **Conseil** : Soyez sûr que tous les TCP et ports UDP exigés pour permettre à Expressway-C pour fonctionner correctement sont ouverts dans le FW B, juste comme spécifié dans ce document Cisco : Utilisation de port IP de Cisco Expressway pour la traversée de Pare-feu

Vérifiez

Packet Tracer peut être utilisé sur l'ASA pour confirmer que les travaux de traduction NAT statique d'Expressway-e au besoin.

Packet Tracer pour tester 64.100.0.10 à TCP/5222 :

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This example shows only when Static one-to-one NAT is used.

static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

Packet Tracer pour tester 64.100.0.10 à TCP/8443 :

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This example shows only when Static one-to-one NAT is used.

static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

Packet Tracer pour tester 64.100.0.10 à TCP/5061.

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This example shows only when Static one-to-one NAT is used.

static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

Packet Tracer pour tester 64.100.0.10 à UDP/24000 :

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This example shows only when Static one-to-one NAT is used.

static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

Packet Tracer pour tester 64.100.0.10 à UDP/36002 :

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This example shows only when Static one-to-one NAT is used.

static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

Dépannez

Étape 1. Comparez les captures de paquet.

Des captures de paquet peuvent être prises au d'entrée et aux interfaces de sortie ASA

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This example shows only when Static one-to-one NAT is used.

static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

Captures de paquet pour 64.100.0.10 à TCP/5222 :

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This example shows only when Static one-to-one NAT is used.

static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

Captures de paquet pour 64.100.0.10 à TCP/5061 :

```
! Static PAT for a Range of Ports is Not Possible - A configuration line is required per port.
This example shows only when Static one-to-one NAT is used.

static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

Étape 2. Examinez les captures accélérées de paquet de baisse de chemin de Sécurité (ASP).

Les captures de baisse d'ASP ASA prennent les paquets que l'ASA a décidé de relâcher. L'option **toute** capture tous les possibles raison pourquoi l'ASA a relâché un paquet. Ceci peut être rétréci vers le bas s'il y a n'importe quelle raison suspectée. Pour une liste de raisons qu'une ASA l'utilise pour classifier ces baisses, exécutez la **baisse d'asp d'exposition de** commande

La mémoire tampon par défaut pour chaque capture ASA est 512 KO. S'il y a beaucoup de paquets relâché par cette ASA, cette mémoire tampon sera remplie très rapidement. Cette mémoire tampon peut être incrémentée utilisant la **mémoire tampon d'**option.

```
capture asp type asp-drop all

show cap asp

OR

show cap asp | i 64.100.0.10
show cap asp | i 10.0.10.2
```

> **Conseil** : Il est très utile dans ce scénario confirmer cette capture d'ASP ASA si l'ASA relâche des paquets dus à un ACL manquant ou NAT (qui est nécessaire pour ouvrir un TCP ou un port UDP spécifique pour Expressway-e).

Recommandations

Assurez-vous que l'inspection SIP/H.323 est complètement désactivée sur les Pare-feu impliqués

Il est fortement recommandé pour désactiver le SIP et H.323 l'inspection sur les Pare-feu qui traitent le trafic réseau à ou d'Expressway-e. Une fois activée, l'inspection SIP/H.323 s'avère fréquemment pour affecter négativement la fonctionnalité intégrée de traversée d'Expressway firewall/NAT.

C'est un exemple de la façon désactiver le SIP et H.323 les inspections sur l'ASA :

```
capture asp type asp-drop all

show cap asp

OR

show cap asp | i 64.100.0.10
show cap asp | i 10.0.10.2
```

Solution alternative

Une solution alternative à mettre en application Expressway-e utilisant de doubles interfaces réseau/double NIC est d'implémenter Expressway-e avec un NIC simple et NAT statique utilisant la configuration NAT de réflexion sur les Pare-feu. Ce lien affiche d'autres détails au sujet de ce scénario :

> **Note**: Pendant qu'on lui mentionnait au début de ce document, la double implémentation NIC est recommandée au-dessus de la réflexion NAT.

Documentation associée

Cisco Expressway-e et Expressway-C - Guide de déploiement de configuration de base

Plaçant un VCS Expressway de Cisco dans un DMZ plutôt que dans l'Internet public

Utilisation de port IP de Cisco Expressway pour la traversée de Pare-feu