ASA 8.0.4/8.2.1 et configuration CUBE pour autoriser les appels vidéo aux points de terminaison vidéo Internet

Contenu

Introduction

Ce document fournit des informations sur la façon dont utiliser l'appliance de sécurité adaptable (ASA) et le Logiciel Cisco Unified Border Element (CUBE) pour faciliter des appels vidéos aux points finaux visuels basés par Internet.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

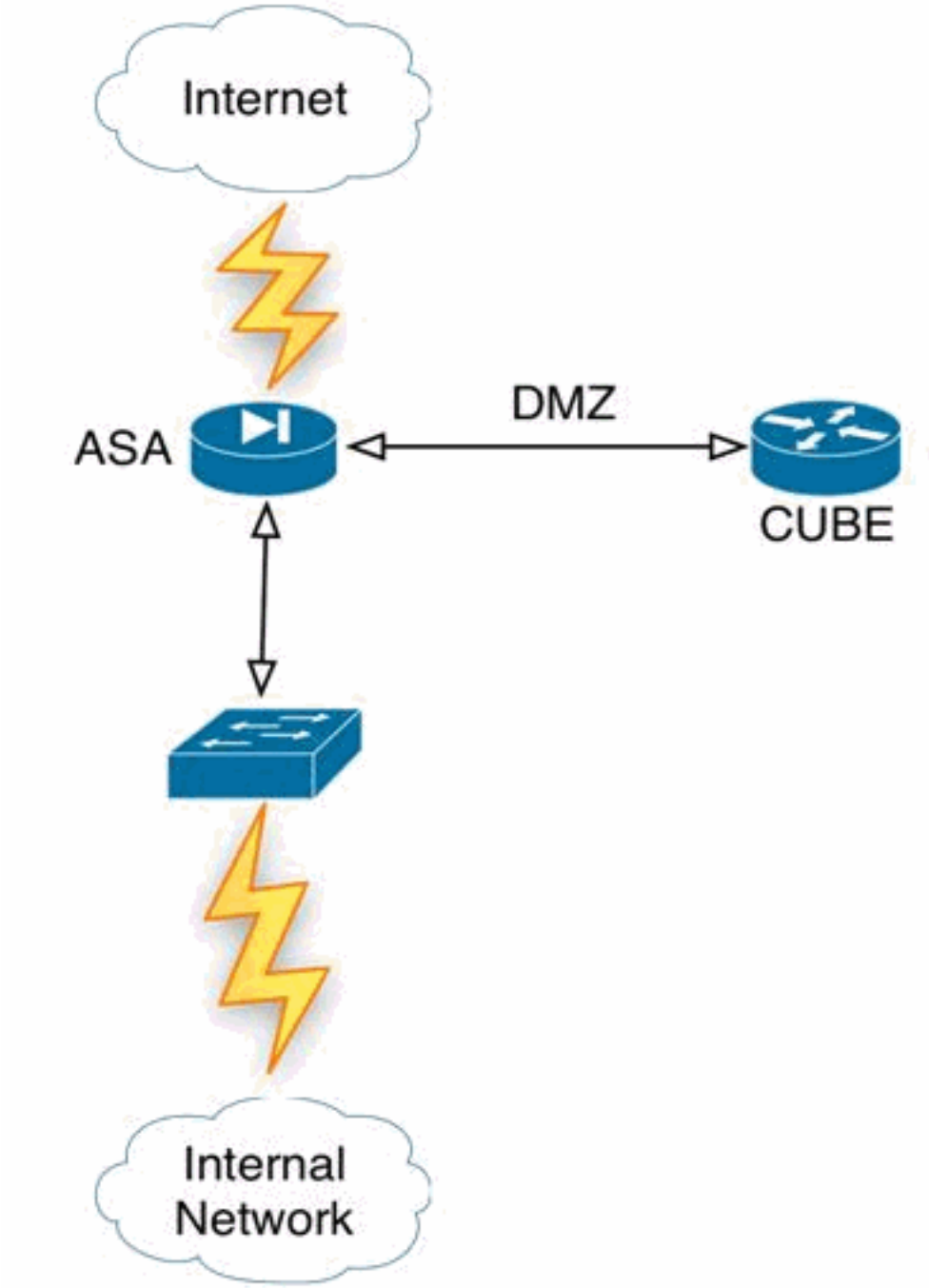
Informations générales

Ce document adresse utiliser l'ASA et le CUBE pour faciliter des appels vidéos aux points finaux visuels basés par Internet. Des appels vidéos sont initiés des points finaux visuels s'arrêtant outre du CUBE quand le CUBE est déployé sur l'interface DMZ de l'ASA.

Note: Ceci adresse une configuration trouvant en ce qui concerne NAT sur l'ASA quand le CUBE est déployé sur le DMZ. Le test a prouvé que cette situation n'affecte pas des réseaux où le CUBE

est déployé sur l'interface interne de l'ASA.

C'est la topologie du réseau générique qui devrait être mise en référence dans tout ce document :



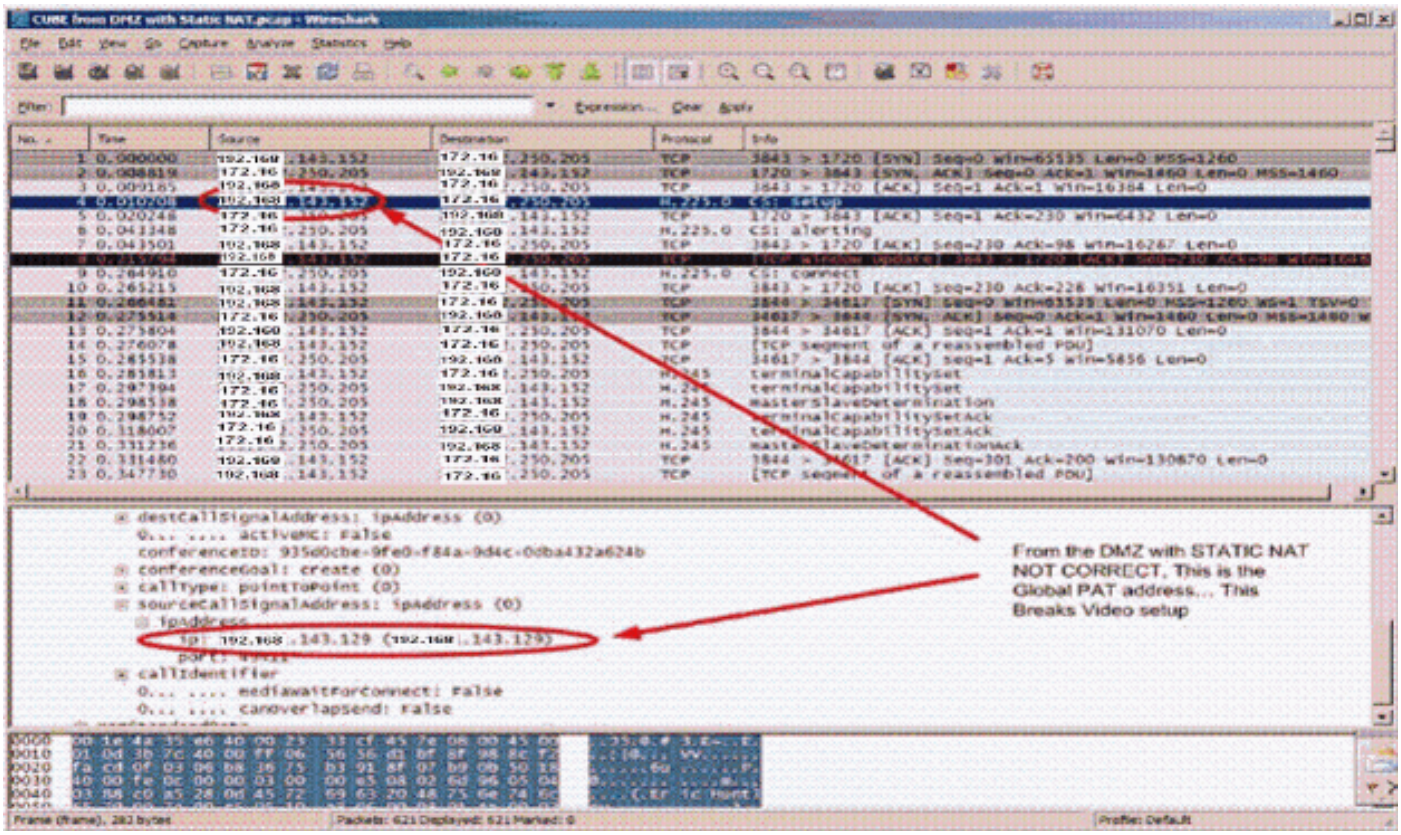
En utilisant des périphériques vidéos de n'importe quelle interface autre que l'interface interne et en initiant une session vidéo sortante (par l'interface extérieure), on doit observer un certain nombre de mises en garde de configuration pour qu'une session vidéo fonctionne correctement de ces interfaces.

Il y a une condition qui se produit où l'ASA 8.0.4 et 8.2.1, engine de H.323 utilisera l'adresse configurée « de PAT global » dans le champ Paquet d'installation de CS des « sourceCallSignalAddress » quand une session vidéo est initiée d'une interface « DMZ » tandis qu'un NAT statique superposant est configuré de l'interface interne à cela interface DMZ. Cette condition n'effectue pas des sessions vidéo initiées de l'intérieur à l'extérieur utilisant un NAT statique d'hôte, alors que la ligne ci-dessous est en place.

```
Static (inside,DMZ) 172.20.0.0 172.20.0.0 netmask 255.255.0.0
```

Pour illustrer plus loin cette question, le tir d'écran suivant indique que l'adresse IP contenue dans le domaine de « sourceCallSignalAddress » n'apparie pas l'adresse IP de l'expéditeur (NAT statique configuré pour ce périphérique). Au lieu de cela l'adresse IP appartient à l'adresse globale de PAT qui est configurée.

Ceci casse une session vidéo.



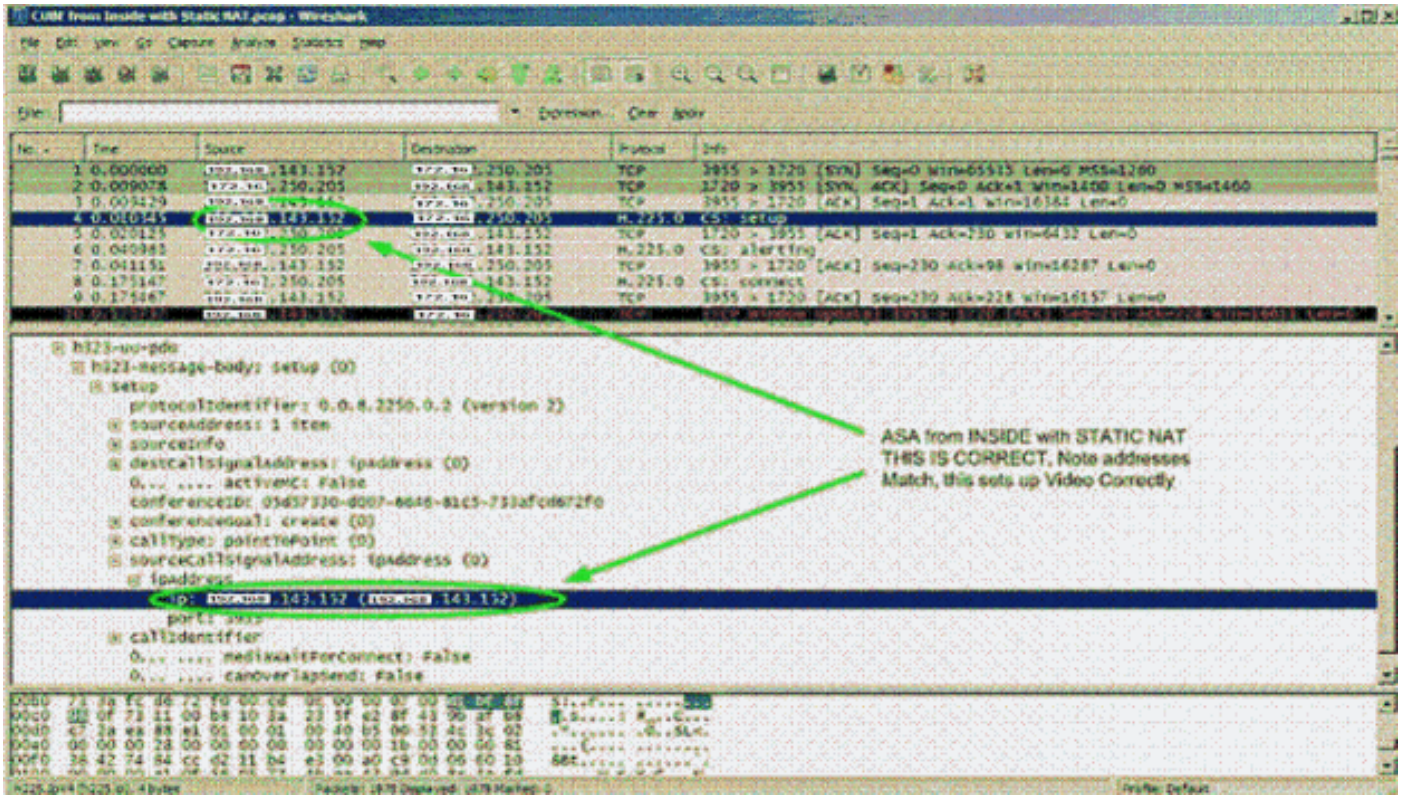
La déclaration de traduction NAT statique pour le périphérique en tant que configuré est comme suit :

```
static (dmz,outside) 192.168.143.152 172.20.220.20 netmask 255.255.255.255
```

Là où 172.20.220.0/24 est le réseau utilisé pour l'interface DMZ. Superpositions du cet espace IP avec ce qui suit :

```
Static (inside,DMZ) 172.20.0.0 172.20.0.0 netmask 255.255.0.0
```

Superposer NAT statique n'effectue pas à l'intérieur des sessions vidéo.



Dans ce tir d'écran, une session vidéo utilisant la même traduction NAT statique qui a été utilisée dans l'exemple précédent qui a provenu de l'interface DMZ est vue.

```
static (dmz,outside) 192.168.143.152 172.20.15.20 netmask 255.255.255.255
```

Comme indiqué dans le tir d'écran ci-dessus, les sourceCallSignalAddress apparie l'adresse IP de l'expéditeur et est correctement traduits par l'engine de H.323. La déclaration NAT statique superposante récapitulée n'effectue pas des sessions vidéo initiées et originaires de l'interface réseau intérieure.

Contournement

Afin d'initier correctement des sessions vidéo d'une interface DMZ exige que l'adresse IP l'un ou l'autre soit complètement différente des espaces réseau intérieurs utilisés, par exemple dans ce cas pas une partie de l'espace d'adressage 172.20.0.0/16 ; ou soyez exclu par l'intermédiaire des traductions NAT statiques de l'intérieur au DMZ.

Exemple :

```
static (inside,dmz) 172.20.0.0 172.20.0.0 netmask 255.255.128.0
static (inside,dmz) 172.20.128.0 172.20.128.0 netmask 255.255.192.0
static (inside,dmz) 172.20.192.0 172.20.192.0 netmask 255.255.240.0
static (inside,dmz) 172.20.208.0 172.20.208.0 netmask 255.255.248.0
static (inside,dmz) 172.20.216.0 172.20.216.0 netmask 255.255.252.0
static (inside,dmz) 172.20.222.0 172.20.222.0 netmask 255.255.255.0
static (inside,dmz) 172.20.223.0 172.20.223.0 netmask 255.255.255.0
static (inside,dmz) 172.20.224.0 172.20.224.0 netmask 255.255.224.0
```

Ces déclarations NAT statiques comportent l'espace 172.20.0.0/16 entier excepté l'espace 172.20.220.0/24.

Il est essentiel en tant qu'élément de la conception où un périphérique visuel de proxy tel que le

CUBE est placé dans un environnement DMZ, cette statique superposante soit pris en considération.

Le test de développement de Cisco informe que ce n'est pas une bogue ou un comportement anormal pour cette configuration et est développé par conception.

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Assistance technique concernant la technologie vocale
- Assistance concernant les produits vocaux et de communications unifiées
- Support et documentation techniques - Cisco Systems