Exemple de configuration CUBE (Unified Border Element) avec IVR de Vidéoconférence Unifiée (CUVC)

Contenu

Introduction

L'adoption des communications vidéo basées sur IP au sein de l'entreprise est bien en cours. Dans l'environnement, le vidéo économiques d'aujourd'hui d'utilisation de clients plus fréquemment comme outil pour des transmissions internes à l'entreprise avec les avantages principaux de cette adoption étant gains dans la productivité des employés et les efficacités opérationnelles.

La plupart des réseaux de communications vidéo basés sur IP d'entreprise sont aujourd'hui comme des îles relativement à d'autres tels réseaux d'entreprise interconnectés utilisant une technologie plus ancienne d'Integrated Services Digital Network (le RNIS). Le RNIS est très utilisé généralement pour toute la supplémentaire-entreprise ou transmission de supplémentaire-campus avec d'autres entreprises et, dans certains cas, même avec les filiales distantes au sein de l'entreprise elle-même. Les avantages d'une grande portée des communications vidéo basées sur IP peuvent vraiment être réalisés avec la connectivité IP de bout en bout dans ou entre des organismes pour faciliter des transmissions d'entreprise à entreprise (de commerce électronique interentreprises). Ceci exige une transition du RNIS aux solutions basées sur IP qui traversent l'Internet au lieu du PSTN, activant une option convergée moins chère pour des transmissions internes à l'entreprise et de commerce électronique interentreprises.

La transition en gros des circuits RNIS aux connexions IP par l'intermédiaire de l'Internet n'est pas une entreprise insignifiante. Les circuits RNIS, et les passerelles visuelles qui attachent le RNIS dans les communications vidéo basées sur IP monde, sont des solutions largement déployées, temps-prouvées et de confiance. En dépit des limites en facilitant les services de communications

vidéo de la deuxième génération, le RNIS fixe toujours la norme par rapport à laquelle de nouvelles solutions sont mesurées en prenant dans la Sécurité, l'intimité, la facturation, et la démarcation de considération. Les nouvelles solutions doivent offrir les assurances semblables de niveau de services pour que des entreprises et des fournisseurs de services les considèrent comme alternative viable. Les entreprises ont besoin ainsi d'une manière de mettre à jour tous les avantages associés avec le RNIS tout en exploitant les efficacités d'étendre les communications vidéo basées sur IP au delà de l'entreprise.

Cet exemple de configuration met en valeur les caractéristiques du Logiciel Cisco Unified Border Element (CUBE) et montre spécifiquement comment le CUBE prend en charge la capacité pour un point final qui réside quelque part sur l'Internet pour composer par l'intermédiaire d'une adresse IP à une unité de contrôle multipoint (MCU) ou au point final qui sont derrière un Pare-feu entreprise. Cette fonctionnalité présente la caractéristique de *priorité de null-called-number* disponible dans la release 12.4(22)YB du CUBE 1.3 et la fonctionnalité RVI disponible dans la release 5.6 de Cisco Unified Videoconferencing (CUVC) MCU. Ce document contient des recommandations de configuration et des points de départ possibles pour des entreprises s'embarquant sur cette évolution.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- La connaissance de base de la façon configurer et utiliser le Cisco IOS expriment (comme des pairs de cadran)
- Connaissance de base de la façon configurer et utiliser le CUBE
- Compréhension de base de la façon dont les Pare-feu fonctionnent

Composants utilisés

Les informations dans ce document sont basées en fonction :

- Logiciel Cisco Unified Border Element et garde-porte de Cisco IOS qui s'exécute sur un routeur de Cisco 2800 et utilise la version de Cisco IOS 12.4.22(YB) ou la Cisco IOS version 15.0.1M
- Solution de la vidéoconférence 3545 IP de Cisco qui exécute la version de logiciel 5.6 ou 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 opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

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

Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Note: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce diagramme affiche à CUBE des points finaux externes introduisant sécurisé dans le réseau client par l'intermédiaire d'une adresse IP interne de point final.

Écoulement d'appel de diagramme

1. Un point final externe sur l'Internet compose une adresse IP publique de CUBE (192.168.1.2) pour joindre une conférence vidéo qui réside sur une unité de contrôle multipoint interne de Cisco (MCU). H.323 les messages d'établissement d'appel arrivent au CUBE en vertu d'un premier *trou d'épingle* pour le port TCP 1720 configuré dans l'appliance de sécurité adaptable Cisco (ASA) qui est le Pare-feu qui fournit la borne de Sécurité pour le réseau. Dans cet exemple, le CUBE a une adresse IP privée ainsi l'adresse publiquement routable visée par le point final extérieur est le résultat d'un NAT statique (traduction d'adresses réseau) exécuté par l'ASA.**Note**: Pour l'illustration, Cisco utilise seulement des espaces adresses d'adresse IP privée dans la documentation.
2. Puisque le message de configuration entrant n'inclut pas les chiffres composés habituels par lesquels le CUBE viserait normalement le prochain tronçon de l'appel, le CUBE utilise les chiffres (1234567890) configurés par la commande de configuration de **priorité de null-called-number**. Utilisant cette adresse, les messages d'établissement d'appel poursuivent vers le réseau client interne.
3. L'ASA a deux trous d'épingle pour prendre en charge cette étape de l'appel : un pour permettre à CUBE à la consultation l'adresse désirée par l'intermédiaire de la caractéristique interne de garde-porte CUVC-M et un pour permettre au message de configuration résultant du CUBE pour obtenir à CUVC-M d'établir l'appel au MCU basé sur l'adresse E.164 configurée dans le pair de cadran sur le CUBE. Utilisant H.323 la caractéristique d'inspection sur l'ASA, la signalisation et les medias restants circulent des connexions de TCP et UDP sont ouverts dynamiquement selon les informations glanées de la signalisation d'établissement d'appel.
4. Le garde-porte interne CUVC-M conduit l'appel à l'IPVC-MCU qui inclut une nouvelle caractéristique du vidéo RVI qui présente un menu graphique d'options à l'utilisateur externe. Ce menu est navigué en écrivant des tonalités DTMF par l'intermédiaire du clavier de numérotation ou à télécommande du point final appelant. L'utilisateur final sélectionne simplement l'ID de conférence de l'*option du menu de conférence de joindre* et entre alors le mot de passe nécessaire si configuré.
5. Le point final visuel interne joint la conférence en composant le même ID de conférence que le point final externe.

Configurations

Ce document utilise les configurations suivantes :

- Exemple de configuration de CUBE
- Exemple de configuration ASA

Configuration de CUBE

```
!
version 12.4
service timestamps debug datetime localtime
service timestamps log datetime msec
service password-encryption
service sequence-numbers
!
hostname cube1
!
boot-start-marker
boot system flash:c2800nm-adventerprisek9_ivs-mz.124-
22.YB.bin
boot-end-marker
!
ip source-route
!
!
multilink bundle-name authenticated
!
!
!
voice service voip
  allow-connections h323 to h323
  h323
  emptycapability
  null-called-number override 1234567890
  h225 start-h245 on-connect
  call start slow
  h245 passthru all
!
!
!
voice class h323 10
!
!
voice-card 0
!
!
!
!
interface GigabitEthernet0/0
 ip address 172.16.1.100 255.255.255.0
 ip route-cache same-interface
 duplex auto
 speed auto
 h323-gateway voip interface
 h323-gateway voip id vgk1 ipaddr 172.16.1.100 1719
priority 1
!--- vgk1 defines zone the cube to register with the
local Gatekeeper service h323-gateway voip h323-id cube1
!--- Defines the ID of CUBE h323-gateway voip tech-
prefix 1# h323-gateway voip bind srcaddr 172.16.1.100 !
! ip forward-protocol nd ip route 0.0.0.0 0.0.0.0
172.16.1.1 ip http server no ip http secure-server ! ! !
! dial-peer voice 1 voip destination-pattern .T !--- To
match outbound call leg to send to GK process session
target ras incoming called-number . !--- For inbound
```

```
call leg codec transparent ! ! gateway timer receive-rtp
1200 ! ! ! gatekeeper zone local vgk1 cisco.com zone
remote CUVCM cisco.com 10.1.1.26 invia vgk1 outvia vgk1
enable-intrazone zone prefix CUVCM 1234567890 gw-type-
prefix 1#* default-technology no use-proxy GK1 default
inbound-to terminal no use-proxy GK1 default outbound-
from terminal bandwidth interzone default 1000000 no
shutdown ! end
```

Configuration ASA

```
ASA Version 8.2(1)
!
!--- This is only a portion of the ASA config. !--- In a
typical production scenario, these commands would !---
be in addition to the current security policies
configured. ! interface Ethernet0/0 no nameif no
security-level no ip address ! interface Ethernet0/0.2
vlan 2 nameif inside security-level 100 ip address
10.1.1.1 255.255.255.0 ! interface Ethernet0/0.12 vlan
12 nameif dmz security-level 50 ip address 172.16.1.1
255.255.255.0 ! interface Ethernet0/0.500 vlan 500
nameif outside security-level 0 ip address 192.168.1.2
255.255.255.0 ! boot system disk0:/asa821-k8.bin ftp
mode passive clock timezone CDT -6 access-list dmz-in
extended permit icmp any any access-list dmz-in extended
permit udp host 172.16.1.100any eq 1719 access-list dmz-
in extended permit tcp host 172.16.1.100any eq h323 !---
The access list allows CUBE address lookups and call !--
- signaling respectively to get to the interior of the
network. ! access-list outside access in extended permit
icmp any any access-list outside access in extended
permit tcp any host 192.168.1.2 eq h323 access-list
outside access in extended permit udp any host
192.168.1.2 eq 1719 !--- The access list allows exterior
call setups and address !--- look ups respectively to
get to the CUBE. ! ! access-list inside-to-DMZ-exemption
extended permit ip 10.0.0.0 255.0.0.0 10.150 .150.0
255.255.255.0 !--- This access list prevents the global
NAT translation intended !--- for the outside interface
from being used on the conversations !--- between
internal endpoints and CUBE. ! mtu inside 1500 mtu dmz
1500 mtu outside 1500 nat-control global (outside) 1
192.168.1.5-192.168.1.100 netmask 255.255.255.0 !---
Note that the general NAT pool should not overlap the !-
-- ASA interface nor the static NAT used for CUBE. ! nat
(inside) 0 access-list inside-to-DMZ-exemption nat
(inside) 1 0.0.0.0 0.0.0.0 nat (dmz) 1 172.168.1.0
255.255.255.0 static (dmz,outside) 192.168.1.2
172.16.1.100 netmask 255.255.255.255 !--- The previous
statement is what establishes the publicly !--- routed
address for CUBE on the outside interface. ! access-
group dmz-in in interface dmz access-group
outside access in in interface outside route inside
10.0.0.0 255.255.255.0 10.1.1.2 1 route outside 0.0.0.0
0.0.0.0 192.168.1.254 1 !--- These two static route
statements assume the existence of !--- a next hop
router on both inside and outside interfaces. ! timeout
xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00
udp 0:10:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323
0:10:00 h225 1:00:00 mgcp 0:10:00 mgcp-pat 0:10:00 !---
Note: It is a good idea to increase the H.225 timeout.
Not all endpoints !--- send enough traffic on this
```

```
connection to keep it alive. The H.225 command !---
includes the H.245 attributes.

!
policy-map global_policy
 class inspection_default
  inspect h323 h225
  inspect h323 ras
```

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Cette image affiche le garde-porte de Cisco IOS étant ajouté au Gestionnaire de vidéoconférence unifiée Cisco. Le modèle de garde-porte de Cisco IOS est sélectionné dans la liste déroulante.

Cette image affiche la vérification chez la section de gestion des ressources du gestionnaire de vidéoconférence de Cisco Unified que le garde-porte de Cisco IOS a été ajouté avec succès. Voici que vous pouvez voir le contrôleur d'accès H.323 de Cisco IOS répertorié avec l'adresse IP de 172.16.1.100.

Cette image affiche la configuration de réception automatique dans la vidéoconférence de Cisco Unified qui affiche l'adresse e.164 (1234567890) qui correspondent au numéro appelé nul configuré sur le CUBE.

Ce les images affiche ce que le vidéo RVI de Cisco IPVC renverra au point final visuel appelant. Utilisant le contrôle à télécommande ou de pavé numérique du point final visuel, l'utilisateur choisit une téléconférence vidéo par l'intermédiaire de DTMF (intrabande) qui est hébergé sur le CUVC MCU et joint la téléconférence vidéo appropriée.

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
- Dépannage des problèmes de téléphonie IP Cisco
- Support et documentation techniques - Cisco Systems