Configuration de routeur élémentaire avec Cisco Configuration Professional

Contenu

Introduction

Ce document décrit comment utiliser Cisco Configuration Professional (Cisco CP) afin de définir la configuration de base du routeur. La configuration de base du routeur inclut la configuration de l'adresse IP, le routage par défaut, la charge statique et le routage dynamique, le NATing statique et dynamique, le nom d'hôte, la bannière, le mot de passe secret, les comptes utilisateurs, et d'autres options. Cisco CP te permet pour configurer votre routeur dans plusieurs environnements de réseau, tels que le petit bureau à domicile de bureau (SOHO), la succursale (BO), le bureau régional, et le lieu d'exploitation principal ou les sièges sociaux d'entreprise, avec une interface facile à utiliser de gestion basée sur le Web.

Pour plus d'informations sur le Cisco Configuration Professional, référez-vous au guide de démarrage rapide de Cisco Configuration Professional.

Conditions préalables

Composants utilisés

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

Routeur de Cisco 2811 avec la version de logiciel 12.4(9) de Cisco IOS®

Version 2.5 de Cisco CP

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.

Installez le Cisco Configuration Professional

Exécutez ces étapes afin d'installer le CCP :

Téléchargez Cisco CP V2.5 du centre logiciel Cisco (clients enregistrés seulement) et installez-le sur votre ordinateur local.

La dernière version de Cisco CP peut être trouvée au site Web CCP.

Lancez Cisco CP de votre ordinateur local par le **début** > les **programmes** > le **Cisco Configuration Professional** et choisissez la **Communauté** qui a le routeur que vous voulez configurer.

Afin de découvrir le périphérique que vous voulez configurer, mettre en valeur le routeur et cliquer sur le bouton de **découvrir**.

Note: Pour les informations sur les modèles de routeur de Cisco et les releases IOS qui sont compatibles à CCPv2.5, référez-vous à la section compatible de releases de Cisco IOS.

Note: Pour les informations sur les conditions requises PC qui exécutent CCPv2.5, référez-vous à la section de configurations système requises

Configuration de routeur pour diriger Cisco CP

Exécutez ces étapes de configuration afin de diriger Cisco CP sur un routeur de Cisco :

Connectez à votre routeur utilisant le telnet, SSH, ou par la console.

Entrez le mode de configuration globale utilisant cette commande :

```
Router(config)#enable
Router(config)#
```

Si le HTTP et les HTTPS sont activés et configurés utiliser des numéros du port non standard, vous pouvez ignorer cette étape et simplement utiliser le numéro de port déjà configuré.

Activez le serveur de HTTP ou HTTPS de routeur utilisant ces commandes de logiciel de Cisco IOS :

```
Router(config)# ip http server
Router(config)# ip http secure-server
Router(config)# ip http authentication local
```

Créez un utilisateur avec le niveau de privilège 15 :

```
Router(config)# username <username> privilege 15 password 0 <password>
```

Note: Remplacez le *<username>* et le *<password>* par le nom d'utilisateur et mot de passe que vous voulez configurer. N'utilisez pas le même mot de passe pour vos mots de passe d'utilisateur et d'enable.

Configurez le SSH et le telnet pour le niveau 15 de procédure de connexion locale et de privilège.

```
Router(config)# line vty 0 4
Router(config-line)# privilege level 15
Router(config-line)# login local
Router(config-line)# transport input telnet
Router(config-line)# transport input telnet ssh
Router(config-line)# exit
```

(Facultatif) activez les gens du pays se connectant pour prendre en charge la fonction de surveillance de log :

```
Router(config)# logging buffered 51200 warning
```

Conditions requises

Ce document suppose que le routeur de Cisco est complètement opérationnel et configuré pour permettre à Cisco CP pour apporter des modifications de configuration.

Pour des informations complètes sur la façon commencer utilisant Cisco CP, référez-vous à obtenir commencé par le Cisco Configuration Professional.

Conventions

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

Configurez

Dans cette section, vous êtes présenté avec les informations pour configurer les paramètres de base pour un routeur dans un réseau.

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 document utilise la configuration réseau suivante :

Note: Les schémas d'adressage d'IP utilisés dans cette configuration ne sont pas légalement routables sur Internet. Ce sont des adresses RFC 1918 qui ont été utilisés dans un environnement de laboratoire.

Configuration d'interface

Exécutez ces étapes afin de configurer les interfaces d'un routeur de Cisco :

Cliquez sur **à la maison** afin d'aller à Cisco CP la page d'accueil.

La page d'accueil de Cisco CP fournit des informations telles que le matériel et le logiciel du routeur, de la disponibilité des fonctionnalités, et d'un résumé de configuration.

Choisissez **configurent > Gestion > interfaces d'interface et les connexions > créent la connexion** afin de configurer la connexion WAN pour l'interface.

Comme exemple, pour FastEthernet 0/1, choisissez l'option d'**Ethernets** et cliquez Create New Connection.

Note: Pour d'autres types d'interfaces comme des **Ethernets**, choisissez le type d'interface respective et cliquez Create New Connection pour poursuivre.

Cliquez sur Next afin de poursuivre une fois que cette interface apparaît :

Choisissez **FastEthernet 0/1** (désiré) de l'option d'interfaces disponible et cliquez sur Next.

Spécifiez l'adresse IP statique avec le masque de sous-réseau correspondant pour l'interface et cliquez sur **Next**.

Configurez le routage par défaut avec des paramètres optionnels tels que la prochaine adresse IP de saut (172.16.1.2 selon le schéma de réseau) fournie par l'ISP et cliquez sur Next.

Cette fenêtre apparaît et montre le récapitulatif de configuration configuré par l'utilisateur. Cliquez sur **Finish** (Terminer).

Note: La Connectivité de la configuration peut être vérifiée en vérifiant la case à cocher à côté du **test la Connectivité après avoir configuré**. C'est une fonctionnalité facultative disponible.

Cette fenêtre apparaît et montre l'état de livraison de la commande au routeur. Sinon, elle affiche des erreurs si la livraison de la commande échoue en raison de commandes incompatibles ou des fonctions non prises en charge.

Choisissez **configurent > Gestion > interfaces d'interface et les connexions > éditent des interfaces/connexions** afin d'ajouter/les éditent/effacements les diverses interfaces.

Sélectionnez l'interface avec laquelle vous souhaitez faire des modifications et cliquez sur **Edit** si vous voulez modifier la configuration de l'interface. Ici, vous pouvez changer l'adresse IP statique existante.

Configuration NAT

Configuration NAT dynamique

Exécutez ces étapes afin de configurer le NAT dynamique dans un routeur de Cisco :

Choisissez **configurent > routeur > lancement NAT > de base NAT** et de clic la **tâche sélectionnée** afin de configurer NATing de base.

Cliquez sur **Next** (Suivant).

Choisissez l'interface qui se connecte à l'Internet ou à votre ISP et choisissez la plage d'adresses IP avec laquelle l'accès Internet doit être partagé. Après avoir choisi ces informations, cliquez sur Next comme affiché ici :

Cette fenêtre apparaît et montre le récapitulatif de configuration configuré par l'utilisateur. Cliquez sur **Finish** (Terminer).

La fenêtre Edit NAT Configuration montre la configuration NAT dynamique avec l'adresse IP traduite surchargée (fonction PAT). Si vous voulez configurer le NAT dynamique avec un pool d'adresse, cliquez sur **Address Pool**.

Cliquez sur **Add**.

Ici, les informations telles que le nom du pool et la plage d'adresses IP avec le netmask sont fournies. Il peut y avoir des périodes où la majeure partie des adresses du pool ont été affectées et où le pool d'adresses IP est presque épuisé. Quand cela se produit, la fonction PAT peut être utilisée avec une adresse IP unique afin de satisfaire les demandes supplémentaires d'adresses IP. Activez la case **Port Address Translation (PAT)** si vous voulez que le routeur utilise la fonction PAT lorsque le pool d'adresses est presque épuisé.

Cliquez sur **OK**.

Cliquez sur **Add**.

Cliquez sur **Edit**.

Choisissez le **pool d'adresses** dans le champ de type, fournissez le nom au pool d'adresses comme **groupe**, et cliquez sur OK.

Cette fenêtre montre la configuration de la fonction NAT dynamique avec le pool d'adresses. Cliquez sur **Designate NAT Interfaces**.

Utilisez cette fenêtre afin de désigner les interfaces internes et externes que vous voulez utiliser dans les traductions NAT. La fonction NAT utilise les désignations d'intérieur et d'extérieur quand elle interprète des règles de traduction parce que les traductions sont effectuées de l'intérieur vers l'extérieur, ou de l'extérieur vers l'intérieur.

Une fois désignées, ces interfaces sont utilisées dans toutes les règles de traduction NAT. Les interfaces désignées apparaissent au-dessus de la liste de règles de traduction (Translation Rules) dans la fenêtre NAT principale.

Configuration NAT statique

Exécutez ces étapes afin de configurer NAT statique dans un routeur de Cisco :

Choisissez **configurent > routeur > NAT > éditent la configuration NAT** et cliquent sur Add afin de configurer NATing statique.

Choisissez la **direction** de l'intérieur à extérieur ou de l'externe vers interne, et spécifiez l'adresse IP intérieure à traduire dessous **se traduisent de l'interface**. Pour que le **traduire relie la** zone, choisissez le type :

Choisissez **IP Address** si vous voulez que l'adresse Translate from Address soit traduite en une adresse IP définie dans la zone IP Address.

Choisissez **Interface** si vous voulez que l'option **Translate from Address** utilise l'adresse d'une interface sur le routeur. L'adresse **Translate from Address** est traduite dans l'adresse IP affectée à l'interface que vous spécifiez dans la zone Interface.

Activez la case à cocher **Redirect Port** si vous voulez inclure les informations sur le port pour le périphérique interne dans la traduction. Cela vous permet d'utiliser la même adresse IP publique pour plusieurs périphériques, à condition qu'un port différent soit spécifié pour chaque périphérique. Vous devez créer une entrée pour chaque mappage de ports pour cette adresse traduite (Translated to). Cliquez sur **TCP** s'il s'agit d'un numéro de port TCP et cliquez sur **UDP** s'il s'agit d'un numéro de port UDP. Dans la zone Original Port, entrez le numéro du port sur le périphérique interne. Dans la zone Translated Port, entrez le numéro

du port que le routeur doit utiliser pour cette traduction. Référez-vous à la section Permettre à l'Internet d'accéder à des périphériques internes de la rubrique Configurer la traduction d'adresses de réseau : Mise en route.

Cette fenêtre affiche la configuration statique de NATing avec la redirection de port activée :

Acheminement de la configuration

Configuration du routage statique

Exécutez ces étapes afin de configurer le routage statique dans un routeur de Cisco :

Choisissez **configurent > routeur > charge statique et routage dynamique** et cliquent sur Add afin de configurer le routage statique.

Introduisez l'adresse réseau de destination avec le masque et choisissez l'interface sortante ou la prochaine adresse IP de saut.

Cette fenêtre affiche la route statique configurée pour le réseau de 10.1.1.0 avec 172.16.1.2 comme prochaine adresse IP de saut :

Configuration du routage dynamique

Exécutez ces étapes afin de configurer le routage dynamique dans un routeur de Cisco :

Choisissez **configurent > routeur > charge statique et routage dynamique**.

Sélectionnez **RIP** et cliquez sur **Edit**.

Vérifiez le **RIP d'enable**, choisissez la version RIP, et cliquez sur Add.

Spécifiez l'adresse réseau à annoncer.

Cliquez sur **OK**.

Cliquez sur **Deliver** pour transférer les commandes au routeur.

Cette fenêtre affiche la configuration dynamique de routage de RIP :

Configuration - Divers

Exécutez ces étapes afin de configurer les autres paramètres de base dans un routeur de Cisco :

Choisissez **configurent > routeur > options de routeur** et cliquent sur Edit si vous voulez

changer les propriétés d'adresse Internet, de nom de domaine, de bannière, et d'enable secret password pour un routeur.

Choisissez **configurent > routeur Access > comptes utilisateurs/vue** afin d'ajouter/éditent/effacements les comptes utilisateurs au routeur.

Choisissez **configurent > des utilitaires > configuration en cours de sauvegarde au PC** afin de sauvegarder la configuration au NVRAM du routeur aussi bien qu'au PC et remettre à l'état initial la configuration en cours pour transférer des configurations (d'usine).

Note: Afin d'employer le CCP pour restaurer le fichier de configuration stocké sur un ordinateur sur un routeur ou sauvegarde le fichier de configuration d'un routeur à un ordinateur, pour accéder à l'éditeur de configuration, et le clic que **je conviens**. Dans la fenêtre de configurer, choisissez la **configuration d'importation du PC**, et puis cliquez sur le bouton de **configuration en cours de remplacer**.

Configuration CLI

Configuration du routeur

```
Router#show run
Building configuration...

Current configuration : 2525 bytes
! version 12.4 service timestamps debug datetime msec
service timestamps log datetime msec no service
password-encryption ! hostname Router ! boot-start-
marker boot-end-marker ! no logging buffered enable
password cisco ! no aaa new-model ! resource policy ! !
! ip cef ! ! ! !--- RSA certificate generated after you
enable the !--- ip http secure-server command.

crypto pki trustpoint TP-self-signed-2401602417
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2401602417
 revocation-check none
 rsakeypair TP-self-signed-2401602417

crypto pki certificate chain TP-self-signed-2401602417
 certificate self-signed 01
  30820248 308201B1 A0030201 02020101 300D0609 2A864886
F70D0101 04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967
6E65642D 43657274
  69666963 6174652D 32343031 36303234 3137301E 170D3130
30353139 30393031
  31315A17 0D323030 31303130 30303030 305A3031 312F302D
06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361
74652D32 34303136
  30323431 3730819F 300D0609 2A864886 F70D0101 01050003
818D0030 81890281
  8100CD35 A3A6E322 9B6005DA A0FF26C2 8A0DC5AF 27B38F3B
DBF2BF58 D8F2655D
  31115681 EC8BC750 03FE3A25 0F79DC74 3A839496 CB9486F1
A1F5BF43 D92BA7AF
  3C72A57B D8D37799 50493588 A5A18F7F 27955AB0 AC36B560
```

```
3BE9F648 A4F6F41F
  B9E9C5E6 F9570DEB 5555FDED 9593BD00 5ABB30CD D3B9BDFA
F570F987 651652CE
  3D310203 010001A3 70306E30 0F060355 1D130101 FF040530
030101FF 301B0603
  551D1104 14301282 10526F75 7465722E 70616D6D 692E636F
6D301F06 03551D23
  04183016 80146A0A C2100122 EFDA58AB C319820D 98256622
52C5301D 0603551D
  0E041604 146A0AC2 100122EF DA58ABC3 19820D98 25662252
C5300D06 092A8648
  86F70D01 01040500 03818100 83B0EC8C 6916178F 587E15D6
5485A043 E7BB258D
  0C9A63F2 DA18793D CACC026E BC0B9B33 F8A27B34 5BD7DD7F
FCECA34F 04662AEC
  07FD7677 A90A8D1C 49042963 C2562FEC 4EFFF17C 360BF88A
FEDC7CAA AE308F6C
  A5756C4A F574F5F3 39CE14AE BAAEC655 D5920DD0 DA76E296
B246E36E 16CFBC5A
  00974370 170BBDAD C1594013
  quit


! ! ! ! ! ! ! ! !--- Create a user account named ccpccp
with all privileges.

username ccpccp privilege 15 password 0 cisco123
archive
 log config
  hidekeys

! ! ! ! ! ! !--- The LAN interface configured with a
private IP address. interface FastEthernet0/0
description $ETH-LAN$ ip address 192.168.1.1
255.255.255.0 !--- Designate that traffic that
originates from behind !--- the interface is subject to
Network Address Translation (NAT).  ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto

! !--- This is the LAN interface configured with a
routable (public) IP address. interface FastEthernet0/1
description $ETH-WAN$ ip address 172.16.1.1
255.255.255.0 !--- Designate that this interface is the
!--- destination for traffic that has undergone NAT. ip
nat outside
 ip virtual-reassembly
duplex auto
 speed auto

! ! !--- RIP version 2 routing is enabled. router rip
version 2 network 192.168.1.0 no auto-summary !--- This
is where the commands to enable HTTP and HTTPS are
configured. ip http server ip http authentication local
ip http secure-server ! !--- This configuration is for
dynamic NAT. !


!--- Define a pool of outside IP addresses for NAT. ip
nat pool pool 10.10.10.1 10.10.10.100 netmask
255.255.255.0 !--- In order to enable NAT of the inside
source address, !--- specify that traffic from hosts
that match access list 1 !--- are NATed to the address
```

```
pool named pool1. ip nat inside source list 1 pool pool1
! !--- Access list 1 permits only 122.168.1.0 network to
be NATed. access-list 1 remark CCP_ACL Category=2
access-list 1 permit 192.168.1.0 0.0.0.255 ! !--- This
configuration is for static NAT !--- In order to
translate the packets between the real IP address
10.10.10.1 with TCP !--- port 80 and the mapped IP
address 172.16.1.1 with TCP port 500. !

ip nat outside source static tcp 10.10.10.1 8080
172.16.1.1 80 extendable
! ! ! ! !--- The default route is configured and points
to 172.16.1.2. ip route 0.0.0.0 0.0.0.0 172.16.1.2 ! ! !
! control-plane ! ! ! ! ! ! ! ! ! ! line con 0 line aux
0 !--- Telnet enabled with password as cisco. line vty 0
4 password cisco transport input all line vty 5 15
password cisco transport input all ! ! ! end
```

Vérifiez

Choisissez **Configure > Interface & Connections > Edit Interface Connections > Test Connection** pour tester la connectivité de bout en bout. Vous pouvez spécifier l'adresse IP de l'extrémité distante si vous cliquez sur la case d'option **User-specified**.

Dépannez

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

Note: Reportez-vous à Informations importantes sur les commandes de débogage avant d'émettre des commandes **debug**.

Vous pouvez utiliser ces options afin de dépanner :

Choisissez l'**aide > au sujet de ce routeur** afin de visualiser le matériel et les détails du logiciel du routeur.

L'option d'**aide** fournit des informations au sujet des diverses options disponibles à Cisco CP pour la configuration des Routeurs.

Comment est-ce que je peux changer le nom d'utilisateur et le mot de passe pour le routeur ?

Vous pouvez changer le nom et le mot de passe d'utilisateur du routeur par Cisco CP. Terminez-vous ces étapes afin de changer le nom d'utilisateur et le mot de passe :

Créez un nouveau compte utilisateur provisoire, et puis ouvrez une session au compte utilisateur provisoire.

Changez le nom d'utilisateur et le mot de passe du compte utilisateur principal (c'est-à-dire, le compte utilisateur du routeur sur lequel vous voulez changer le nom d'utilisateur et le mot

de passe) à votre Cisco CP.

Déconnectez-vous du compte provisoire, et de la procédure de connexion au compte utilisateur principal.

Supprimez le compte utilisateur provisoire après que vous changiez le mot de passe pour le compte principal.

Je reçois une erreur interne quand j'utilise l'Internet Explorer 8 pour accéder à Cisco CP. Comment faire pour résoudre ce problème ?

Problème

Vous pourriez recevoir cette erreur interne quand vous utilisez l'Internet Explorer 8 pour configurer le routeur de gamme 2800 utilisant Cisco CP :

```
Erreur interne : [Fault= de FaultEvent [le faultString= " Send de défaut RPC a manqué » erreur
NetConnection.Call.Failed Channel.Connect.Failed de faultDetail= la " " Client.Error.MessageSend
de faultCode= » : HTTP : État 200 : URL : cancelable=true eventPhase=2] de bubbles=false de "
défaut » de type= 'http://localhost:8600/messagebroker/amf'"] messageId="A08846FF-E7C6-F578-
7C38-61C6E94899C7"
```

Déclassifiant Javas ne résout pas le problème.

Solution

Cette erreur pourrait être le résultat d'un problème de compatibilité de navigateur. L'Internet Explorer 8 change beaucoup d'aspects fondamentaux des demandes se développantes d'IE. Cisco recommande que vous déclassifiiez l'Internet Explorer à la version 7. Vous devriez également désinstaller et réinstaller Cisco CP.

Je reçois ce message d'erreur quand j'essaye d'installer Cisco CP : « Incapable de lire le fichier source. Le fichier a pu être corrompu. Veuillez réinstaller le Cisco Configuration Professional pour résoudre le problème. » Comment faire pour résoudre ce problème ?

Problème

Quand vous téléchargez le fichier de configuration et la tentative d'application d'installer Cisco CP, vous pourriez recevoir cette erreur :

```
Router#show run
Building configuration...

Current configuration : 2525 bytes
! version 12.4 service timestamps debug datetime msec service timestamps log datetime msec no
service password-encryption ! hostname Router ! boot-start-marker boot-end-marker ! no logging
buffered enable password cisco ! no aaa new-model ! resource policy ! ! ! ip cef ! ! ! !--- RSA
certificate generated after you enable the !--- ip http secure-server command.

crypto pki trustpoint TP-self-signed-2401602417
```

```
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2401602417
 revocation-check none
 rsakeypair TP-self-signed-2401602417

crypto pki certificate chain TP-self-signed-2401602417
 certificate self-signed 01
  30820248 308201B1 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 32343031 36303234 3137301E 170D3130 30353139 30393031
  31315A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32 34303136
  30323431 3730819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100CD35 A3A6E322 9B6005DA A0FF26C2 8A0DC5AF 27B38F3B DBF2BF58 D8F2655D
  31115681 EC8BC750 03FE3A25 0F79DC74 3A839496 CB9486F1 A1F5BF43 D92BA7AF
  3C72A57B D8D37799 50493588 A5A18F7F 27955AB0 AC36B560 3BE9F648 A4F6F41F
  B9E9C5E6 F9570DEB 5555FDED 9593BD00 5ABB30CD D3B9BDFA F570F987 651652CE
  3D310203 010001A3 70306E30 0F060355 1D130101 FF040530 030101FF 301B0603
  551D1104 14301282 10526F75 7465722E 70616D6D 692E636F 6D301F06 03551D23
  04183016 80146A0A C2100122 EFDA58AB C319820D 98256622 52C5301D 0603551D
  0E041604 146A0AC2 100122EF DA58ABC3 19820D98 25662252 C5300D06 092A8648
  86F70D01 01040500 03818100 83B0EC8C 6916178F 587E15D6 5485A043 E7BB258D
  0C9A63F2 DA18793D CACC026E BC0B9B33 F8A27B34 5BD7DD7F FCECA34F 04662AEC
  07FD7677 A90A8D1C 49042963 C2562FEC 4EFFF17C 360BF88A FEDC7CAA AE308F6C
  A5756C4A F574F5F3 39CE14AE BAAEC655 D5920DD0 DA76E296 B246E36E 16CFBC5A
  00974370 170BBDAD C1594013
  quit


! ! ! ! ! ! ! ! !--- Create a user account named ccpccp with all privileges.

username ccpccp privilege 15 password 0 cisco123
archive
 log config
  hidekeys

! ! ! ! ! ! !--- The LAN interface configured with a private IP address. interface
FastEthernet0/0 description $ETH-LAN$ ip address 192.168.1.1 255.255.255.0 !--- Designate that
traffic that originates from behind !--- the interface is subject to Network Address Translation
(NAT).  ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto

! !--- This is the LAN interface configured with a routable (public) IP address. interface
FastEthernet0/1 description $ETH-WAN$ ip address 172.16.1.1 255.255.255.0 !--- Designate that
this interface is the !--- destination for traffic that has undergone NAT. ip nat outside
 ip virtual-reassembly
duplex auto
 speed auto

! ! !--- RIP version 2 routing is enabled. router rip version 2 network 192.168.1.0 no auto-
summary !--- This is where the commands to enable HTTP and HTTPS are configured. ip http server
ip http authentication local ip http secure-server ! !--- This configuration is for dynamic NAT.
!


!--- Define a pool of outside IP addresses for NAT. ip nat pool pool 10.10.10.1 10.10.10.100
netmask 255.255.255.0 !--- In order to enable NAT of the inside source address, !--- specify
that traffic from hosts that match access list 1 !--- are NATed to the address pool named pool1.
 ip nat inside source list 1 pool pool1 ! !--- Access list 1 permits only 122.168.1.0 network to
be NATed. access-list 1 remark CCP_ACL Category=2 access-list 1 permit 192.168.1.0 0.0.0.255 !
!--- This configuration is for static NAT !--- In order to translate the packets between the
```

```
real IP address 10.10.10.1 with TCP !--- port 80 and the mapped IP address 172.16.1.1 with TCP
port 500. !

ip nat outside source static tcp 10.10.10.1 8080 172.16.1.1 80 extendable
! ! ! ! !--- The default route is configured and points to 172.16.1.2. ip route 0.0.0.0 0.0.0.0
172.16.1.2 ! ! ! ! control-plane ! ! ! ! ! ! ! ! ! ! line con 0 line aux 0 !--- Telnet enabled
with password as cisco. line vty 0 4 password cisco transport input all line vty 5 15 password
cisco transport input all ! ! ! end
```

Solution

Essayez le suivant afin de résoudre ceci.

Supprimez tous les exemples de Cisco CP sur votre PC, et exécutez un téléchargement frais et l'installez.

Si l'étape précédente ne fonctionne pas, essayer de télécharger une différente version de Cisco CP.

Si l'étape précédente ne fonctionne pas, contacter Cisco TAC.

Note: Vous devez avoir les qualifications valides d'utilisateur Cisco afin de contacter Cisco TAC.

Comment est-ce que j'accède aux logs techniques de Cisco CP ?

Le début de clic **> programme > Cisco Systems > Cisco Configuration Professional > collectent des données pour le support technique**. Cisco CP archive automatiquement les logins un fichier zip nommé *_ccptech.zip. Exécutez un* système de fichier local recherchent ce fichier s'il n'est pas enregistré à votre appareil de bureau. Vous pouvez envoyer ces logs techniques à CiscoTAC pour davantage de dépannage.

Note: Clôturez tous les exemples de Cisco CP pour se débarasser de toutes les autres questions en archivant les logs.

La détection de routeur prend plus de temps que d'habitude. Comment faire pour résoudre ce problème ?

Problème

Une fois que Cisco CP est lancé et la communauté est configurée, la détection du routeur prend plus de temps que d'habitude. Voici les logs de Cisco CP qui décrivent le temps se sont écoulés :

```
Router#show run
Building configuration...

Current configuration : 2525 bytes
! version 12.4 service timestamps debug datetime msec service timestamps log datetime msec no
service password-encryption ! hostname Router ! boot-start-marker boot-end-marker ! no logging
buffered enable password cisco ! no aaa new-model ! resource policy ! ! ! ip cef ! ! ! !--- RSA
certificate generated after you enable the !--- ip http secure-server command.

crypto pki trustpoint TP-self-signed-2401602417
```

```
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2401602417
 revocation-check none
 rsakeypair TP-self-signed-2401602417

crypto pki certificate chain TP-self-signed-2401602417
 certificate self-signed 01
  30820248 308201B1 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 32343031 36303234 3137301E 170D3130 30353139 30393031
  31315A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32 34303136
  30323431 3730819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100CD35 A3A6E322 9B6005DA A0FF26C2 8A0DC5AF 27B38F3B DBF2BF58 D8F2655D
  31115681 EC8BC750 03FE3A25 0F79DC74 3A839496 CB9486F1 A1F5BF43 D92BA7AF
  3C72A57B D8D37799 50493588 A5A18F7F 27955AB0 AC36B560 3BE9F648 A4F6F41F
  B9E9C5E6 F9570DEB 5555FDED 9593BD00 5ABB30CD D3B9BDFA F570F987 651652CE
  3D310203 010001A3 70306E30 0F060355 1D130101 FF040530 030101FF 301B0603
  551D1104 14301282 10526F75 7465722E 70616D6D 692E636F 6D301F06 03551D23
  04183016 80146A0A C2100122 EFDA58AB C319820D 98256622 52C5301D 0603551D
  0E041604 146A0AC2 100122EF DA58ABC3 19820D98 25662252 C5300D06 092A8648
  86F70D01 01040500 03818100 83B0EC8C 6916178F 587E15D6 5485A043 E7BB258D
  0C9A63F2 DA18793D CACC026E BC0B9B33 F8A27B34 5BD7DD7F FCECA34F 04662AEC
  07FD7677 A90A8D1C 49042963 C2562FEC 4EFFF17C 360BF88A FEDC7CAA AE308F6C
  A5756C4A F574F5F3 39CE14AE BAAEC655 D5920DD0 DA76E296 B246E36E 16CFBC5A
  00974370 170BBDAD C1594013
  quit


! ! ! ! ! ! ! ! !--- Create a user account named ccpccp with all privileges.

username ccpccp privilege 15 password 0 cisco123
archive
 log config
  hidekeys

! ! ! ! ! ! !--- The LAN interface configured with a private IP address. interface
FastEthernet0/0 description $ETH-LAN$ ip address 192.168.1.1 255.255.255.0 !--- Designate that
traffic that originates from behind !--- the interface is subject to Network Address Translation
(NAT).  ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto

! !--- This is the LAN interface configured with a routable (public) IP address. interface
FastEthernet0/1 description $ETH-WAN$ ip address 172.16.1.1 255.255.255.0 !--- Designate that
this interface is the !--- destination for traffic that has undergone NAT. ip nat outside
 ip virtual-reassembly
duplex auto
 speed auto

! ! !--- RIP version 2 routing is enabled. router rip version 2 network 192.168.1.0 no auto-
summary !--- This is where the commands to enable HTTP and HTTPS are configured. ip http server
ip http authentication local ip http secure-server ! !--- This configuration is for dynamic NAT.
!


!--- Define a pool of outside IP addresses for NAT. ip nat pool pool 10.10.10.1 10.10.10.100
netmask 255.255.255.0 !--- In order to enable NAT of the inside source address, !--- specify
that traffic from hosts that match access list 1 !--- are NATed to the address pool named pool1.
 ip nat inside source list 1 pool pool1 ! !--- Access list 1 permits only 122.168.1.0 network to
be NATed. access-list 1 remark CCP_ACL Category=2 access-list 1 permit 192.168.1.0 0.0.0.255 !
!--- This configuration is for static NAT !--- In order to translate the packets between the
```

```
real IP address 10.10.10.1 with TCP !--- port 80 and the mapped IP address 172.16.1.1 with TCP
port 500. !

ip nat outside source static tcp 10.10.10.1 8080 172.16.1.1 80 extendable
! ! ! ! !--- The default route is configured and points to 172.16.1.2. ip route 0.0.0.0 0.0.0.0
172.16.1.2 ! ! ! ! control-plane ! ! ! ! ! ! ! ! ! ! line con 0 line aux 0 !--- Telnet enabled
with password as cisco. line vty 0 4 password cisco transport input all line vty 5 15 password
cisco transport input all ! ! ! end
```

Cette question se produit avec tous les Routeurs indépendamment de leur modèle et plate-forme. En outre, il n'y a aucune mémoire ou questions connexes CPU sur les Routeurs.

Solution

Vérifiez l'authentication mode. Si l'authentification ne se produit pas localement, alors vérifiez s'il y a une question avec le serveur authentifiant. Réparez n'importe quelle question avec le serveur authentifiant afin de résoudre ce problème.

Je ne peux pas visualiser la page de configuration IPS sur Cisco CP. Comment faire pour résoudre ce problème ?

Problème

Quand une caractéristique spécifique dans la fenêtre de configuration n'affiche rien excepté une page vierge, il pourrait y avoir des questions d'une incompatibilité.

Solution

Vérifiez ces éléments afin de résoudre ce problème :

Vérifiez si cette caractéristique spécifique est prise en charge et activée sur votre modèle de routeur.

Vérifiez si vos supports de version de routeur qui comportent. Des incompatibilités de version de routeur ont pu être résolues avec une mise à niveau de la version.

Vérifiez si le problème est avec l'autorisation en cours.

Informations connexes

- Guide de démarrage rapide de Cisco Configuration Professional
- Page d'assistance de produit Cisco - Routeurs
- Page de support NAT
- Support et documentation techniques - Cisco Systems