Configuration d'IPSec sur ADSL sur Cisco 2600/3600 avec ADSL-WIC et modules de chiffrement matériel

Contenu

Introduction

Pendant que l'Internet développe, les succursales exigent que leurs connexions aux lieux d'exploitation principaux sont fiables et sécurisées. Le Réseaux privés virtuels (VPN) protègent les informations entre les bureaux distants et les lieux d'exploitation principaux pendant qu'elles voyagent à travers l'Internet. La sécurité IP (IPSec) peut être utilisée pour garantir que les données qui passent à travers ces VPN sont chiffrées. Le cryptage fournit une autre couche de sécurité des réseaux.

Cette figure affiche un IPSec typique VPN. Un certain nombre de connexions d'Accès à distance et de site à site sont impliquées entre les succursales et les lieux d'exploitation principaux. Habituellement, des liens WAN traditionnels tels que le Relais de trames, le RNIS, et l'accès commuté par modem provisioned entre les sites. Ces connexions peuvent impliquer des frais une fois chers de ravitaillement et des frais mensuels chers. En outre, pour des utilisateurs RNIS et de modem, il peut y avoir de longs temps de connexion.

Le Ligne d'abonné numérique à débit asymétrique (ADSL) offre une alternative illimitée et bonne marchée à ces liens WAN traditionnels. Les données cryptées d'IPSec au-dessus d'une liaison ADSL offrent une connexion sécurisée et fiable et épargnent à des clients l'argent. Une CPE traditionnelle ADSL (CPE) installée dans une succursale exige un modem ADSL qui se connecte à un périphérique qui lance et termine le trafic d'IPSec. Cette figure affiche un réseau typique ADSL.

Le Cisco 2600 et 3600 Routeurs prennent en charge la carte d'interface WAN/ADSL (WIC-1ADSL). Ce WIC-1ADSL est un interarmées et une solution d'accès distant conçu pour répondre aux besoins d'une succursale. L'introduction du WIC-1ADSL et des modules de chiffrement matériel accomplit la demande d'IPSec et le DSL dans une succursale dans une solution de routeur unique. Le WIC-1ADSL élimine le besoin de modem DSL distinct. Le module de chiffrement matériel fournit jusqu'à dix fois la représentation au-dessus du cryptage réservé au logiciel pendant qu'il débarque le cryptage ce des processus du routeur.

Pour plus d'informations sur ces deux Produits, référez-vous aux cartes d'interface WAN/ADSL pour Cisco 1700, 2600, et des routeurs d'accès modulaire de gamme 3700 et des modules de réseau privé virtuel pour Cisco 1700, 2600, 3600, et gamme 3700.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

Routeurs de gamme Cisco 2600/3600 :

- Positionnement Enterprise Plus de la caractéristique 3DES de version de logiciel 12.1(5)YB de Cisco IOS®
- Mo de la DRACHME 64 pour la gamme Cisco 2600, Mo de la DRACHME 96 pour la gamme Cisco 3600
- Le Mo de l'instantané 16 pour la gamme Cisco 2600, flashent 32 Mo pour la gamme Cisco 3600
- WIC-1 ADSL
- Modules de chiffrement matérielAIM-VPN/BP et AIM-VPN/EP pour la gamme Cisco 2600NM-VPN/MP pour Cisco 3620/3640AIM-VPN/HP pour le Cisco 3660

Gamme Cisco 6400 :

- Version du logiciel Cisco IOS 12.1(5)DC1
- MO DE LA MÉMOIRE VIVE DYNAMIQUE 64
- Mo de l'instantané 8

Gamme Cisco 6160 :

- Version du logiciel Cisco IOS 12.1(7)DA2
- MO DE LA MÉMOIRE VIVE DYNAMIQUE 64
- Mo de l'instantané 16

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configurez

Dans cette section, vous êtes présenté avec les informations que vous pouvez employer pour configurer les caractéristiques décrites dans ce document.

Note: Pour obtenir plus d'informations sur les commandes utilisées dans ce document, utilisez l'Outil de recherche de commande (clients enregistrés uniquement).

Diagramme du réseau

Ce document utilise la configuration réseau affichée ce diagramme.

Ce test simule une connexion VPN d'IPSec qui utilise l'ADSL dans un environnement typique de succursale.

Cisco 2600/3600 avec le WIC ADSL et le module de chiffrement matériel forme jusqu'à Cisco 6160 un multiplexeur d'accès de ligne d'abonné numérique (DSLAM). Le Cisco 6400 est utilisé comme périphérique d'agrégation qui termine une session PPP qui initie du routeur de Cisco 2600. Le tunnel d'IPSec commence au CPE 2600 et se termine au Cisco 3600 dans le bureau central, le périphérique de headend d'IPSec dans ce scénario. Le périphérique de headend est configuré pour recevoir des connexions de n'importe quel client au lieu de scruter individuel. Le périphérique de headend est également testé avec seulement des clés pré-partagées et 3DES et processeur de service de périphérie (ESP) - Algorithme de hachage sûr (SHA) - le code d'authentification de message d'information Information (HMAC).

Configurations

Ce document utilise les configurations suivantes :

- Routeur Cisco 2600
- Périphérique de Headend d'IPSec - Routeur de Cisco 3600
- Cisco 6160 DSLAM
- Processeur d'artère de noeud de Cisco 6400 (NRP)

Notez ces points au sujet des configurations :

- Une clé pré-partagée est utilisée. Afin d'installer des sessions d'IPSec aux plusieurs homologues, vous devez définir de plusieurs déclarations de définition principales ou vous devez configurer une crypto-carte dynamique. Si toutes les sessions partagent une clé simple, vous devez utiliser une adresse de pair de 0.0.0.0.
- Le jeu de transformations peut être défini pour l'ESP, l'En-tête d'authentification (AH), ou chacun des deux pour l'Authentification double.
- Au moins une crypto définition des politiques doit être définie par pair. Les crypto map décident le pair pour les utiliser pour créer la session d'IPSec. La décision est basée sur la correspondance d'adresse définie dans la liste d'accès. Dans ce cas, c'est la liste d'accès

101.

- Les crypto map doivent être définis pour les interfaces physiques (interface atm 0/0 dans ce cas) et le virtual-template.
- La configuration présentée dans ce document discute seulement un tunnel d'IPSec au-dessus d'une connexion DSL. Les fonctionnalités de sécurité supplémentaires sont probablement nécessaires afin de s'assurer que votre réseau n'est pas vulnérable. Ces fonctionnalités de sécurité peuvent inclure le Listes de contrôle d'accès (ACL) supplémentaire, le Traduction d'adresses de réseau (NAT), et l'utilisation d'un Pare-feu avec une unité externe ou un ensemble de caractéristiques du pare-feu d'IOS. Chacune de ces caractéristiques peut être utilisée afin de limiter le trafic de non-IPSec à et du routeur.

Routeur Cisco 2600

```
crypto isakmp policy 10
!--- Defines the ISAKMP parameters to be negotiated.
authentication pre-share !--- Defines the pre-shared key
to be exchanged with the peer. crypto isakmp key pre-
shared address 10.1.1.5 ! crypto ipsec transform-set
strong esp-des esp-sha-hmac !--- Defines the transform
set for ESP and/or AH. ! crypto map vpn 10 ipsec-isakmp
set peer 10.1.1.5 set transform-set strong match address
102 !--- Defines the crypto policy that includes the
peer IP address, !--- transform set that is used, as
well as the access list !--- that defines the packets
that are encrypted. ! interface ATM0/0 no ip address atm
vc-per-vp 256 no atm ilmi-keepalive dsl operating-mode
auto no fair-queue ! interface ATM0/0.1 point-to-point
pvc 0/35 encapsulation aal5mux ppp dialer dialer pool-
member 1 ! crypto map vpn !--- Applies the crypto map to
the ATM sub-interface. ! interface FastEthernet0/1 ip
address 1.1.1.1 255.255.255.0 duplex 100 speed full !
interface Dialer1 ip address 10.1.100.101 255.255.255.0
dialer pool 1 encapsulation ppp ppp pap sent-username
2621a password 7 045802150C2E crypto map vpn !---
Applies the crypto map to the Dialer interface. ! ip
classless ! ip route 2.2.2.0 255.255.255.0 10.1.1.5 ip
route 10.1.1.0 255.255.255.0 10.1.100.1 !--- Static
routes between 2600 CPE and IPSec server. ip route
0.0.0.0 0.0.0.0 Dialer1 ! access-list 102 permit ip
1.1.1.0 0.0.0.255 2.2.2.0 0.0.0.255 !--- Access list
that defines the addresses that are encrypted. ! end
```

Périphérique de Headend d'IPSec - Routeur de Cisco 3600

```
crypto isakmp policy 10
!--- Defines the ISAKMP parameters to be negotiated.
authentication pre-share !--- Defines the pre-shared key
to be exchanged with the peer. crypto isakmp key pre-
shared address 10.1.100.101 ! crypto ipsec transform-set
strong esp-des esp-sha-hmac !--- Defines the transform
set for ESP and/or AH. ! crypto map vpn 10 ipsec-isakmp
set peer 10.1.100.101 set transform-set strong match
address 102 !--- Defines the crypto policy that includes
the peer IP address, !--- transform set that are used,
and the access list !--- that defines the packets to be
encrypted. ! interface FastEthernet0/0 ip address
10.1.1.5 255.255.255.0 duplex 100 speed full crypto map
vpn !--- Applies the crypto map to the Fast Ethernet
```

```
interface. ! interface FastEthernet0/1 ip address
2.2.2.1 255.255.255.0 speed full full-duplex ! ip route
1.1.1.0 255.255.255.0 10.1.1.10 ip route 10.1.100.0
255.255.255.0 10.1.1.10 ! access-list 102 permit ip
2.2.2.0 0.0.0.255 1.1.1.0 0.0.0.255 !--- Access list
that defines the addresses to be encrypted. ! end
```

Cisco 6160 DSLAM

```
dsl-profile full
 dmt bitrate maximum fast downstream 10240 upstream 1024
 dmt bitrate maximum interleaved downstream 0 upstream 0
 !
 atm address
47.0091.8100.0000.0004.6dd6.7c01.0004.6dd6.7c01.00
 atm router pnni
 no aesa embedded-number left-justified
 none 1 level 56 lowest
 redistribute atm-static
 !
 interface atm0/0
 no ip address
 atm maxvp-number 0
 atm maxvc-number 4096
 atm maxvci-bits 12
 !
 interface atm 1/2
 no ip address
 dsl profile full
 no atm ilmi-keepalive
 atm soft-vc 0 35 dest-address
 47.0091.8100.0000.0004.c12b.cd81.4000.0c80.8000.00 0 36
 rx-cttr 1 tx-cttr 1
!--- The previous two lines need to be on one line. !---
The network service access point (NSAP) !--- address
comes from the NSP on the Cisco 6400. Issue !--- a show
atm address command.

 !
```

Cisco 6400 NRP

```
dsl-profile full
 dmt bitrate maximum fast downstream 10240 upstream 1024
 dmt bitrate maximum interleaved downstream 0 upstream 0
 !
 atm address
47.0091.8100.0000.0004.6dd6.7c01.0004.6dd6.7c01.00
 atm router pnni
 no aesa embedded-number left-justified
 none 1 level 56 lowest
 redistribute atm-static
 !
 interface atm0/0
 no ip address
 atm maxvp-number 0
 atm maxvc-number 4096
 atm maxvci-bits 12
 !
 interface atm 1/2
 no ip address
 dsl profile full
 no atm ilmi-keepalive
```

```
 atm soft-vc 0 35 dest-address
 47.0091.8100.0000.0004.c12b.cd81.4000.0c80.8000.00 0 36
 rx-cttr 1 tx-cttr 1
!--- The previous two lines need to be on one line. !---
The network service access point (NSAP) !--- address
comes from the NSP on the Cisco 6400. Issue !--- a show
atm address command.

 !
```

Mises en garde

Des connexions ADSL peuvent être configurées avec un virtual-template ou une interface de numérotation.

Une interface de numérotation est utilisée afin de configurer la CPE DSL pour recevoir une adresse du fournisseur de services (l'adresse IP est négociée). Une interface de modèle virtuel est une interface de down-down et ne prend en charge pas l'option négociée d'adresse, qui est nécessaire dans l'environnement DSL. Des interfaces de modèle virtuel ont été au commencement mises en application pour des environnements DSL. Actuellement une interface de numérotation est la configuration recommandée du côté de CPE DSL.

Deux questions sont trouvées au moment de la configuration des interfaces de numérotation avec IPSec :

- ID de bogue Cisco CSCdu30070 (clients enregistrés seulement) — IPSec réservé au logiciel au-dessus de DSL : section de file d'attente d'entrée sur l'interface de numérotation DSL.
- ID de bogue Cisco CSCdu30335 (clients enregistrés seulement) — IPSec réalisé par matériel au-dessus de DSL : section de file d'attente d'entrée sur l'interface de numérotation.

Le contournement en cours pour chacun des deux questions est de configurer la CPE DSL avec l'utilisation de l'interface de modèle virtuel comme décrit dans la configuration.

Des difficultés pour chacun des deux questions sont prévues pour le Logiciel Cisco IOS version 12.2(4)T. Après que cette release, une version mise à jour de ce document soit signalée afin d'afficher la configuration de l'interface du numéroteur en tant qu'autre option.

Vérifiez

Cette section fournit les informations que vous pouvez employer afin de confirmer que votre configuration fonctionne correctement.

Plusieurs **commandes show** peuvent être utilisées afin de vérifier que la session d'IPSec est établie entre les pairs. Les commandes sont nécessaires seulement sur les pairs d'IPSec, dans ce cas les gammes Cisco 2600 et 3600.

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

- **active de connexions de show crypto engine** — Affiche chaque Phase 2 SA établi et le niveau de trafic envoyé.
- **show crypto ipsec sa** — IPSec SA d'expositions construit entre les pairs.

C'est exemple de sortie de commande pour la commande d'**active de connexions de show crypto engine**.

```
show crypto engine connections active

ID   Interface        IP-Address   State Algorithm           Encrypt Decrypt
1    <none>           <none>       set   HMAC_SHA+DES_56_CB  0       0
200 Virtual-Template1 10.1.100.101 set   HMAC_SHA            0       4
201 Virtual-Template1 10.1.100.101 set   HMAC_SHA            4       0
```

C'est exemple de sortie de commande pour la commande de **show crypto ipsec sa**.

```
show crypto ipsec sa

Interface:  Virtual-Template1
Crypto map tag: vpn, local addr. 10.1.100.101

Local ident (addr/mask/prot/port):  (1.1.1.0/255.255.255.0/0/0)
Remote ident (addr/mask/prot/port): (2.2.2.0/255.255.255.0/0/0)
Current_peer:  10.1.1.5
 PERMIT, flags= {origin_is_acl,}
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr failed: 0, # pkts decompress failed: 0
#send errors 11, #recv errors 0

local crypto endpt:  10.1.100.101, remote crypto endpt.: 10.1.1.5
path mtu 1500, media mtu 1500
current outbound spi:  BB3629FB

inbound esp sas:
spi:  0x70C3B00B(1891872779)
 transform: esp-des, esp-md5-hmac
 in use settings ={Tunnel,}
 slot: 0, conn id: 2000, flow_id: 1, crypto map: vpn
 sa timing: remaining key lifetime (k/sec): (4607999/3446)
 IV size: 8 bytes
 Replay detection support: Y

Inbound ah sas:

Inbound pcp sas:

Outbound esp sas:
Spi: 0xBB3629FB(3140889083)
 Transform: esp-des, esp-md5-hmac
 In use settings ={Tunnel,}
 Slot:0, conn id: 2001, flow_id: 2, crypto map: vpn
 Sa timing: remaining key lifetime (k/sec): (4607999/3446)
 IV size: 8bytes
 Replay detection support: Y

Outbound ah sas:

Outbound pcp sas:
```

Dépannez

Cette section fournit les informations que vous pouvez employer afin de dépanner votre configuration.

`Le « état de modem = le` message de `0x8"` qui est signalé par la commande de **debug atm events** signifie habituellement que le WIC1-ADSL ne peut pas recevoir la Détection Onde Porteuse du DSLAM connecté. Dans cette situation, les besoins des clients de vérifier que le signal DSL provisioned sur les deux fils moyens relativement au connecteur RJ11. Quelques compagnies de téléphone provision le signal DSL sur les broches de l'extérieur deux à la place.

Dépannage des commandes

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

Note: Avant d'émettre des commandes **debug**, reportez-vous à Informations importantes sur les commandes de débogage.

Attention : N'exécutez pas l'élimination des imperfections sur un réseau vivant. Le volume des informations qui affichent peut surcharger votre routeur au point où aucun flux de données et message cpuhog ne sont émis.

- **debug crypto ipsec** — Affiche des événements IPsec.
- **debug crypto isakmp**—Affichage de messages d'événements IKE.

Résumé

L'implémentation d'IPSec au-dessus d'une connexion ADSL fournit une connexion réseau sécurisée et fiable entre les succursales et les lieux d'exploitation principaux. L'utilisation de la gamme Cisco 2600/3600 avec le WIC ADSL et les modules de chiffrement matériel offre plus peu coûteux de la propriété au client pendant que l'ADSL et l'IPSec peuvent maintenant être accomplis dans une solution de routeur unique. La configuration et les mises en garde répertoriées dans ce besoin de papier de servir d'instruction de base pour installer ce type de connexion.

Informations connexes

- Présentation du chiffrement IPSec (IP Security)
- Routeurs de la gamme Cisco 2600
- Réseaux privés virtuels
- Soutien technique DSL et LRE
- Support de Produits de passerelle universelle
- Numérotation et accès de l'assistance technique
- Support technique - Cisco Systems