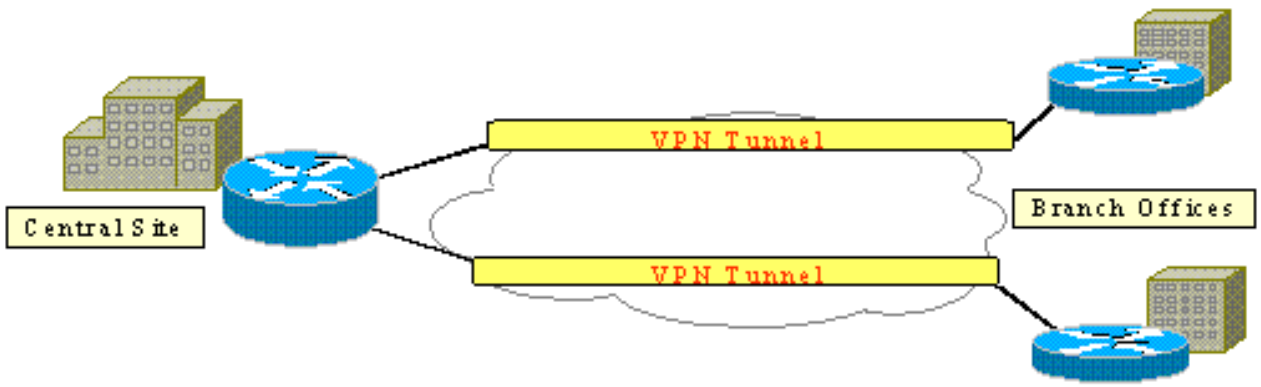
Konfigurieren von IPSec über ADSL auf einem Cisco 2600/3600 mit ADSL-WIC und Hardware-Verschlüsselungsmodulen

Inhalt

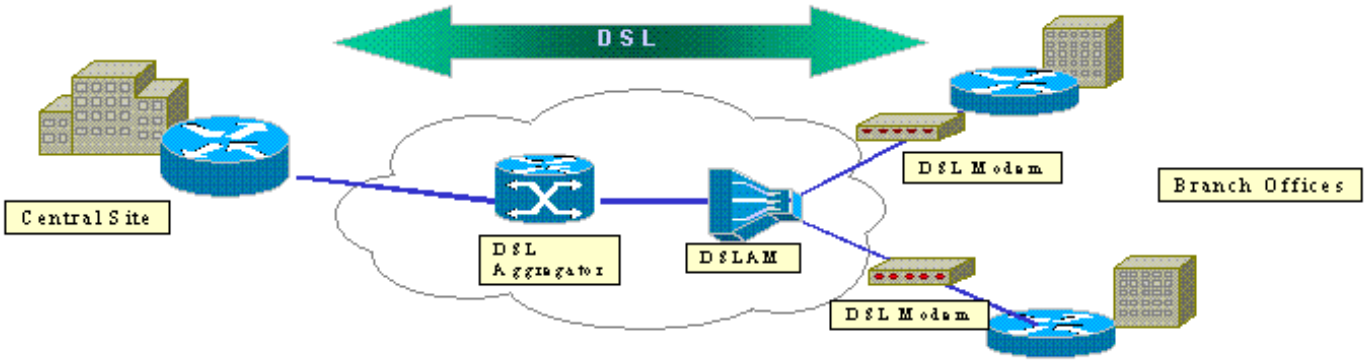
Einführung

Im Zuge der Erweiterung des Internets verlangen Zweigstellen, dass ihre Verbindungen zu den zentralen Standorten zuverlässig und sicher sind. Virtual Private Networks (VPNs) schützen Informationen zwischen Zweigstellen und zentralen Standorten, während sie das Internet durchlaufen. IP Security (IPSec) kann verwendet werden, um sicherzustellen, dass die über diese VPNs übertragenen Daten verschlüsselt werden. Die Verschlüsselung bietet eine weitere Ebene der Netzwerksicherheit.



Diese Abbildung zeigt ein typisches IPSec-VPN. Zwischen den Zweigstellen und den zentralen Standorten sind verschiedene Remote-Zugriffe und standortübergreifende Verbindungen möglich. In der Regel werden zwischen den Standorten herkömmliche WAN-Links wie Frame Relay, ISDN und Modem-Einwahlnummern bereitgestellt. Diese Verbindungen können eine kostspielige einmalige Bereitstellungsgebühr und teure monatliche Gebühren beinhalten. Für ISDN- und Modembenutzer können auch lange Verbindungszeiten bestehen.

ADSL (Asymmetric Digital Subscriber Line) ist eine stets verfügbare, kostengünstige Alternative zu diesen herkömmlichen WAN-Verbindungen. IPSec-verschlüsselte Daten über eine ADSL-Verbindung bieten eine sichere und zuverlässige Verbindung und sparen Kunden Geld. Ein herkömmliches ADSL-Gerät (Customer Premises Equipment, CPE) in einer Zweigstelle erfordert ein ADSL-Modem, das eine Verbindung zu einem Gerät herstellt, das IPSec-Datenverkehr generiert und terminiert. Diese Abbildung zeigt ein typisches ADSL-Netzwerk.



Die Cisco Router 2600 und 3600 unterstützen die ADSL-WAN-Schnittstellenkarte (WIC-1ADSL). Diese WIC-1ADSL ist eine Lösung für Multiservice- und Remote-Zugriff, die speziell auf die Anforderungen von Zweigstellen zugeschnitten ist. Mit der Einführung der WIC-1ADSL- und Hardware-Verschlüsselungsmodule wird der Bedarf an IPSec und DSL in einer Zweigstelle in einer einzigen Router-Lösung erfüllt. Durch WIC-1ADSL ist kein separates DSL-Modem erforderlich. Das Hardware-Verschlüsselungsmodul bietet eine bis zu zehnmal höhere Leistung als die rein softwarebasierte Verschlüsselung, wenn die Verschlüsselung vom Router entlastet wird.

Weitere Informationen zu diesen beiden Produkten finden Sie unter ADSL-WAN-Schnittstellenkarten für die modularen Cisco Access Router der Serien 1700, 2600 und 3700 und Virtual Private Network Modules für die Cisco Serien 1700, 2600, 3600 und 3700 .

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

Cisco Router der Serien 2600 und 3600:

- Cisco IOS® Softwareversion 12.1(5)YB Enterprise PLUS 3DES - Funktionssatz
- DRAM, 64 MB für die Cisco Serie 2600, DRAM, 96 MB für die Cisco Serie 3600
- Flash 16 MB für die Cisco Serie 2600, Flash 32 MB für die Cisco Serie 3600
- WIC-1 ADSL
- Hardware-VerschlüsselungsmoduleAIM-VPN/BP und AIM-VPN/EP für die Cisco Serie 2600NM-VPN/MP für Cisco 3620/3640AIM-VPN/HP für Cisco 3660

Cisco Serie 6400:

- Cisco IOS Softwareversion 12.1(5)DC1
- DRAM, 64 MB
- Flash 8 MB

Cisco Serie 6160:

- Cisco IOS Softwareversion 12.1(7)DA2
- DRAM, 64 MB
- Flash 16 MB

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Sie in einem Live-Netzwerk arbeiten, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen, bevor Sie es verwenden.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Konfiguration

In diesem Abschnitt finden Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten, verwenden Sie das Command Lookup Tool (nur registrierte Kunden).

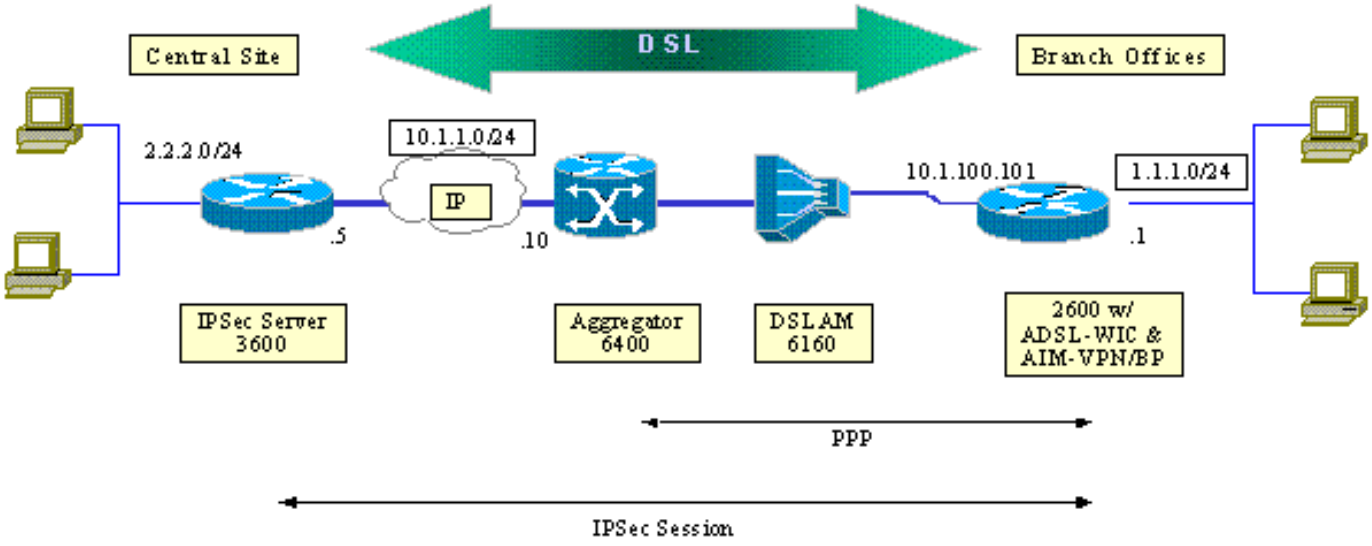
Netzwerkdiagramm

In diesem Dokument wird die in diesem Diagramm dargestellte Netzwerkeinrichtung verwendet.

Dieser Test simuliert eine IPSec-VPN-Verbindung, die ADSL in einer typischen Zweigstellenumgebung verwendet.

Der Cisco 2600/3600 mit ADSL-WIC und Hardware-Verschlüsselungsmodul stellt bis zu einen Cisco 6160 Digital Subscriber Line Access Multiplexer (DSLAM) bereit. Der Cisco 6400 wird als Aggregationsgerät verwendet, das eine PPP-Sitzung beendet, die vom Cisco 2600 Router gestartet wird. Der IPSec-Tunnel stammt vom CPE 2600 und endet beim Cisco 3600 in der Zentrale, in diesem Szenario beim IPSec-Headend. Das Headend-Gerät ist so konfiguriert, dass es Verbindungen von einem beliebigen Client anstelle von individuellen Peering akzeptiert. Das Headend-Gerät wird auch mit vorinstallierten Schlüsseln und dem Hash-basierten Message Authentication Code (HMAC) für den Edge Service Processor (ESP)-Secure Hash Algorithm

(SHA) getestet.



Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

- Cisco Router der Serie 2600
- IPSec-Headend-Gerät - Cisco 3600 Router
- Cisco DSLAM 6160
- Cisco 6400 Node Route Processor (NRP)

Beachten Sie die folgenden Punkte zu den Konfigurationen:

- Ein vorinstallierter Schlüssel wird verwendet. Um IPSec-Sitzungen für mehrere Peers einzurichten, müssen Sie mehrere Schlüsseldefinitionsanweisungen definieren oder eine dynamische Crypto Map konfigurieren. Wenn alle Sitzungen einen Schlüssel gemeinsam nutzen, müssen Sie eine Peer-Adresse von 0.0.0.0 verwenden.
- Der Transformationssatz kann für ESP, den Authentifizierungs-Header (AH) oder beide für die doppelte Authentifizierung definiert werden.
- Pro Peer muss mindestens eine Crypto-Richtliniendefinition definiert werden. Die Crypto-Maps legen fest, welcher Peer zum Erstellen der IPSec-Sitzung verwendet werden soll. Die Entscheidung basiert auf der in der Zugriffsliste definierten Adressenzuordnung. In diesem Fall ist es access-list 101.
- Die Crypto-Maps müssen sowohl für die physischen Schnittstellen (in diesem Fall Schnittstelle ATM 0/0) als auch für die virtuelle Vorlage definiert werden.
- Die in diesem Dokument vorgestellte Konfiguration behandelt nur einen IPSec-Tunnel über eine DSL-Verbindung. Möglicherweise sind zusätzliche Sicherheitsfunktionen erforderlich, um sicherzustellen, dass Ihr Netzwerk nicht verwundbar ist. Zu diesen Sicherheitsfunktionen gehören zusätzliche Zugriffskontrolllisten (ACLs), Network Address Translation (NAT) und die Verwendung einer Firewall mit einer externen Einheit oder einem IOS-Firewall-Feature-Set. Jede dieser Funktionen kann verwendet werden, um Nicht-IPSec-Datenverkehr zum und vom Router einzuschränken.

Cisco Router der Serie 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
```

IPSec-Headend-Gerät - Cisco 3600 Router

```
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 DSLAM 6160

```
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

```
!
username cisco password cisco
!
vc-class atm pppoa
 encapsulation aal5mux ppp Virtual-template1
 !
 interface loopback 0
 ip address 10.1.100.1 255.255.255.0
 !
 interface atm 0/0/0
 no ip address
 no ip route-cache
 no ip mroute-cache
 no atm auto-configuration
 atm ilmi-keepalive 10
 pvc 0/16 ilmi
 !
 hold-queue 1000 in
 !
 interface atm 0/0/0.1 multipoint
 no ip route-cache
 no ip mroute-cach
 class-int pppoa
 pvc 0/36
 !
 interface fast 0/0/0
 ip address 10.1.1.10 255.255.255.0
 no ip route-cache
 no ip mroute-cache
 half-duplex
 !
 interface Virtual-Template1
 ip unnumbered Loopback0
 no ip route-cache
 peer default ip address pool pppoa
 ppp authentication pap chap
```

```
 ppp ipcp accept-address
 ppp multilink
 no ppp multilink fragmentation
 !
 ip local pool pppoa 10.1.100.2 10.1.100.100
 !
```

Hinweise

ADSL-Verbindungen können mit einer virtuellen Vorlage oder einer Dialer-Schnittstelle konfiguriert werden.

Über eine Dialer-Schnittstelle wird das DSL CPE so konfiguriert, dass es eine Adresse vom Service Provider erhält (IP-Adresse wird ausgehandelt). Bei einer Virtual-Template-Schnittstelle handelt es sich um eine Down-Down-Schnittstelle, die die vereinbarte Adressenoption nicht unterstützt, die in der DSL-Umgebung erforderlich ist. Virtual-Template-Schnittstellen wurden ursprünglich für DSL-Umgebungen implementiert. Derzeit wird eine Dialer-Schnittstelle auf der Seite DSL CPE empfohlen.

Zwei Probleme werden bei der Konfiguration der Dialer-Schnittstellen mit IPSec gefunden:

- Cisco Bug-ID CSCdu30070 (nur registrierte Kunden) —Software-only-IPSec über DSL: Eingabewarteschlangen an der DSL-Dialer-Schnittstelle.
- Cisco Bug ID CSCdu30335 (nur registrierte Kunden) - Hardwarebasiertes IPSec über DSL: Eingabewarteschlangen an der Dialer-Schnittstelle.

Die aktuelle Problemumgehung für beide besteht in der Konfiguration des DSL CPE mithilfe der Virtual-Template-Schnittstelle, wie in der Konfiguration beschrieben.

Für die Cisco IOS Software Version 12.2(4)T sind Korrekturen für beide Probleme geplant. Nach dieser Veröffentlichung wird eine aktualisierte Version dieses Dokuments veröffentlicht, um die Konfiguration der Dialer-Benutzeroberfläche als weitere Option anzuzeigen.

Überprüfung

In diesem Abschnitt finden Sie die Informationen, die Sie verwenden können, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Mehrere **show**-Befehle können verwendet werden, um zu überprüfen, ob die IPSec-Sitzung zwischen den Peers eingerichtet wurde. Die Befehle sind nur für IPSec-Peers erforderlich, in diesem Fall für die Cisco Serien 2600 und 3600.

Einige Befehle des Typs **show werden vom Tool** Output Interpreter unterstützt (nur für registrierte Kunden), mit dem sich Analysen der Ausgabe von Befehlen des Typs **show abrufen lassen.**

- **show crypto engine connections active** - Zeigt jede erstellte Phase 2 SA und die Menge des gesendeten Datenverkehrs an.
- **show crypto ipsec sa** - Zeigt IPSec SA, die zwischen Peers erstellt wurde.

Dies ist die Beispielbefehlsausgabe für den Befehl **show crypto engine connections active**.

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
```

Dies ist die Beispielbefehlsausgabe für den Befehl **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:
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Die `Meldung "Modem state = 0x8"`, die durch den Befehl **debug atm events** gemeldet wird, bedeutet in der Regel, dass der WIC1-ADSL keine Carrier Detect von der angeschlossenen DSLAM erhalten kann. In dieser Situation muss der Kunde überprüfen, ob das DSL-Signal an den beiden mittleren Kabeln im Verhältnis zum RJ11-Anschluss bereitgestellt wird. Manche Telcos stellen stattdessen das DSL-Signal auf den beiden äußeren Pins bereit.

Fehlerbehebung bei Befehlen

Einige Befehle des Typs **show werden vom Tool** Output Interpreter unterstützt (nur für registrierte Kunden), mit dem sich Analysen der Ausgabe von Befehlen des Typs **show abrufen lassen.**

Hinweis: Bevor Sie **Debugbefehle** ausgeben, lesen Sie die Informationen Wichtige Informationen über Debug-Befehle.

Vorsicht: Führen Sie kein Debugging in einem Live-Netzwerk aus. Die Informationsmenge, die angezeigt wird, kann Ihren Router so weit überlasten, dass keine Datenflüsse und CPUHOG-Nachrichten ausgegeben werden.

- **debug crypto IPSec**: Zeigt IPSec-Ereignisse an.
- **debug crypto Isakmp**: Zeigt Meldungen über IKE-Ereignisse an.

Zusammenfassung

Die Implementierung von IPSec über eine ADSL-Verbindung bietet eine sichere und zuverlässige Netzwerkverbindung zwischen Zweigstellen und zentralen Standorten. Die Verwendung der Cisco Serien 2600/3600 mit der ADSL-WIC und den Hardware-Verschlüsselungsmodulen bietet Kunden niedrigere Gesamtbetriebskosten, da ADSL und IPSec nun in einer Lösung mit einem Router ausgeführt werden können. Die in diesem Whitepaper aufgeführten Konfigurationen und Probleme müssen als grundlegende Richtlinien für die Einrichtung dieser Art von Verbindung dienen.

Zugehörige Informationen

- Eine Einführung in die IP Security (IPSec)-Verschlüsselung
- Router der Cisco 2600 Serie
- Virtuelle private Netzwerke
- Technischer Support für DSL und LRE
- Unterstützung von Universal Gateways-Produkten
- Unterstützung von DFÜ- und Zugriffstechnologie
- Technischer Support – Cisco Systems