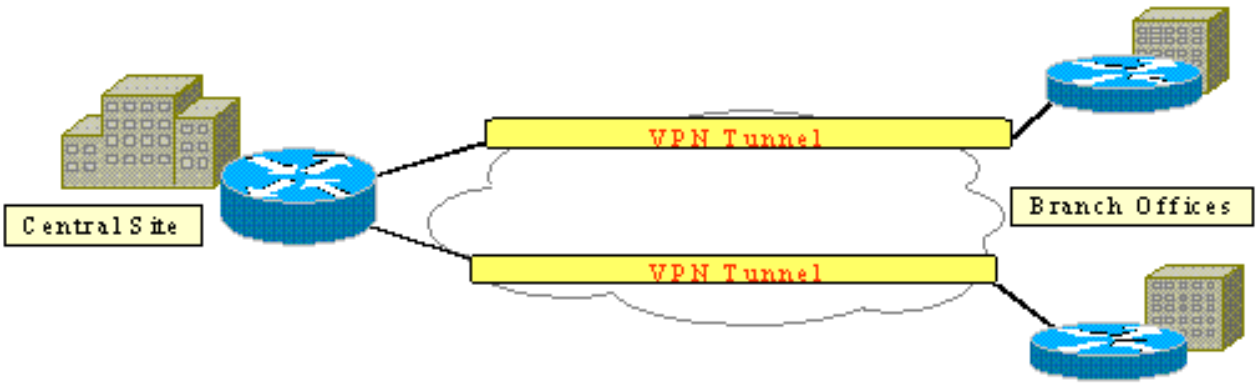
Cisco 2600/3600에서 ADSL-WIC 및 하드웨어 암호화 모듈을 사용하여 IPSec over ADSL 구성

목차

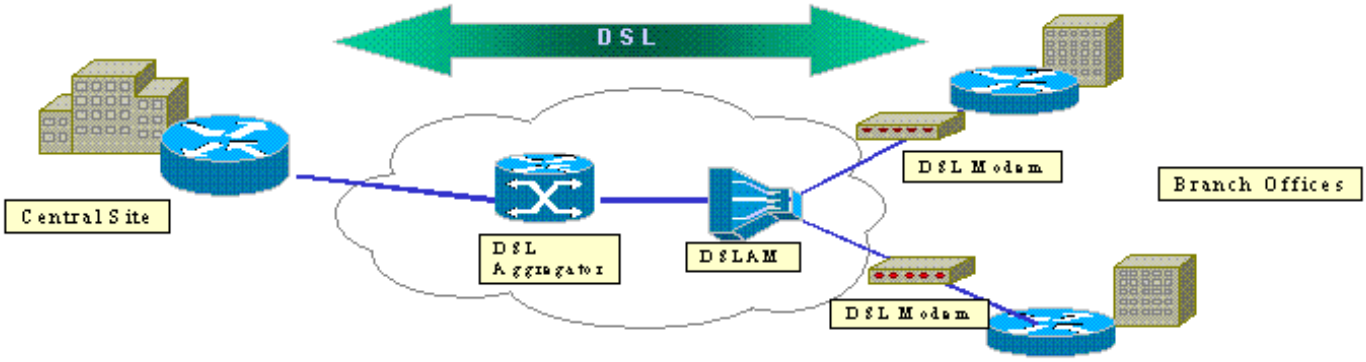
소개

인터넷이 확장됨에 따라 지사에서 중앙 사이트로의 연결이 안정적이고 안전해야 한다고 요구합니다.VPN(Virtual Private Networks)은 인터넷을 통해 원격 사무실과 중앙 사이트 간의 정보를 보호합니다.IPSec(IP Security)을 사용하여 이러한 VPN을 통과하는 데이터가 암호화되도록 할 수 있습니다.암호화는 또 다른 네트워크 보안 계층을 제공합니다.



이 그림에는 일반적인 IPSec VPN이 나와 있습니다.지사와 중앙 사이트 간에는 수많은 원격 액세스 및 사이트 대 사이트 연결이 포함됩니다.일반적으로 사이트 간에 프레임 릴레이, ISDN, 모뎀 전화 접속 등의 기존 WAN 링크가 프로비저닝됩니다.이러한 연결에는 고가의 1회 프로비저닝 비용과 월 비용이 들 수 있습니다.또한 ISDN 및 모뎀 사용자의 경우 연결 시간이 길어질 수 있습니다.

ADSL(Asymmetric Digital Subscriber Line)은 이러한 기존 WAN 링크에 대해 항상 사용 가능한 저렴한 대안을 제공합니다.ADSL 링크를 통한 IPSec 암호화 데이터는 안전하고 신뢰할 수 있는 연결을 제공하며 고객의 비용을 절감합니다.지사에 설치된 기존의 ADSL CPE(Customer Premises Equipment)에는 IPSec 트래픽을 시작 및 종료하는 디바이스에 연결되는 ADSL 모뎀이 필요합니다.이 그림은 일반적인 ADSL 네트워크를 보여줍니다.



Cisco 2600 및 3600 라우터는 ADSL WAN 인터페이스 카드(WIC-1ADSL)를 지원합니다. 이 WIC-1ADSL은 지사의 요구 사항을 충족하도록 설계된 멀티 서비스 및 원격 액세스 솔루션입니다.WIC-1ADSL 및 하드웨어 암호화 모듈이 도입됨에 따라 단일 라우터 솔루션에서 지사에서 IPSec 및 DSL에 대한 수요가 늘어났습니다.WIC-1ADSL을 사용하면 별도의 DSL 모뎀이 필요하지 않습니다.하드웨어 암호화 모듈은 라우터에서 처리하는 암호화를 오프로드할 때 소프트웨어 전용 암호화에 비해 최대 10배의 성능을 제공합니다.

이 두 제품에 대한 자세한 내용은 Cisco 1700, 2600 및 3700 Series Modular Access Router용 ADSL WAN 인터페이스 카드와 Cisco 1700, 2600 및 3700 Series용 Virtual Private Network 모듈을 참조하십시오.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

Cisco 2600/3600 Series 라우터:

- Cisco IOS® Software 릴리스 12.1(5)YB Enterprise PLUS 3DES 기능 집합
- Cisco 2600 시리즈용 DRAM 64MB, Cisco 3600 시리즈용 DRAM 96MB
- Cisco 2600 시리즈용 플래시 16MB, Cisco 3600 시리즈용 플래시 32MB
- WIC-1 ADSL
- 하드웨어 암호화 모듈Cisco 2600 시리즈용 AIM-VPN/BP 및 AIM-VPN/EPCisco 3620/3640용 NM-VPN/MPCisco 3660용 AIM-VPN/HP

Cisco 6400 시리즈:

- Cisco IOS Software 릴리스 12.1(5)DC1

- DRAM 64MB
- 플래시 8MB

Cisco 6160 시리즈:

- Cisco IOS Software 릴리스 12.1(7)DA2
- DRAM 64MB
- 플래시 16MB

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.라이브 네트워크에서 작업하는 경우, 명령을 사용하기 전에 명령의 잠재적인 영향을 이해해야 합니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

구성

이 섹션에서는 이 문서에 설명된 기능을 구성하는 데 사용할 수 있는 정보를 제공합니다.

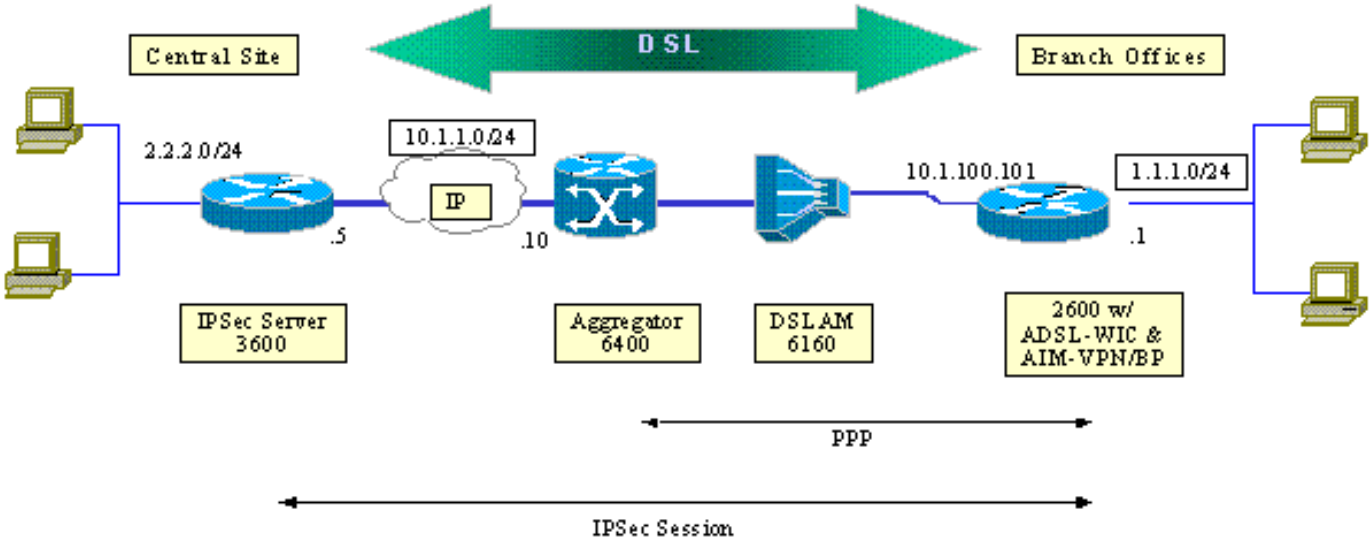
참고: 이 문서에 사용된 명령에 대한 추가 정보를 찾으려면 명령 조회 도구(등록된 고객만 해당)를 사용합니다.

네트워크 다이어그램

이 문서에서는 이 다이어그램에 표시된 네트워크 설정을 사용합니다.

이 테스트는 일반적인 지사 환경에서 ADSL을 사용하는 IPSec VPN 연결을 시뮬레이션합니다.

ADSL-WIC 및 하드웨어 암호화 모듈이 장착된 Cisco 2600/3600은 Cisco 6160 디지털 가입자 회선 액세스 멀티플렉서(DSLAM)까지 교육합니다. Cisco 6400은 Cisco 2600 라우터에서 시작하는 PPP 세션을 종료하는 어그리게이션 디바이스로 사용됩니다.IPSec 터널은 CPE 2600에서 시작되며 중앙 사무실의 Cisco 3600, 즉 이 시나리오의 IPSec 헤드엔드 디바이스에서 종료됩니다.헤드엔드 디바이스는 개별 피어링 대신 모든 클라이언트의 연결을 허용하도록 구성됩니다.헤드엔드 디바이스는 사전 공유 키 및 3DES 및 ESP(Edge Service Processor)-SHA(Secure Hash Algorithm)-HMAC(Hash-based Message Authentication Code)로만 테스트됩니다.



구성

이 문서에서는 다음 구성을 사용합니다.

- Cisco 2600 라우터
- IPSec 헤드엔드 디바이스 - Cisco 3600 라우터
- Cisco 6160 DSLAM
- Cisco 6400 NRP(Node Route Processor)

컨피그레이션에 대한 다음 사항에 유의하십시오.

- 사전 공유 키가 사용됩니다.여러 피어에 IPSec 세션을 설정하려면 여러 개의 키 정의 문을 정의하거나 동적 암호화 맵을 구성해야 합니다.모든 세션이 단일 키를 공유하는 경우 피어 주소 0.0.0.0을 사용해야 합니다.
- 변환 세트는 ESP, AH(Authentication Header) 또는 이중 인증을 위해 둘 다 정의할 수 있습니다 .
- 피어당 하나 이상의 암호화 정책 정의를 정의해야 합니다.암호화 맵은 IPSec 세션을 생성하는 데 사용할 피어를 결정합니다.결정은 액세스 목록에 정의된 주소 일치를 기반으로 합니다.이 경우 access-list 101입니다.
- 암호화 맵은 물리적 인터페이스(이 경우 인터페이스 ATM 0/0) 및 가상 템플릿에 대해 모두 정의해야 합니다.
- 이 문서에 제시된 컨피그레이션에서는 DSL 연결을 통한 IPSec 터널만 설명합니다.네트워크가 취약하지 않도록 하려면 추가 보안 기능이 필요할 수 있습니다.이러한 보안 기능에는 추가 ACL(Access-Control List), NAT(Network Address Translation) 및 외부 장치 또는 IOS 방화벽 기능 집합이 포함된 방화벽 사용이 포함될 수 있습니다.이러한 각 기능을 사용하여 비 IPSec 트래픽을 라우터로 주고받는 것을 제한할 수 있습니다.

Cisco 2600 라우터

```
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 헤드엔드 디바이스 - Cisco 3600 라우터

```
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

```
!
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
 !
```

주의 사항

ADSL 연결은 가상 템플릿 또는 다이얼러 인터페이스로 구성할 수 있습니다.

다이얼러 인터페이스는 DSL CPE가 통신 사업자로부터 주소를 수신하도록 구성하는 데 사용됩니다(IP 주소가 협상됨).가상 템플릿 인터페이스는 다운된 인터페이스이며 DSL 환경에 필요한 협상된 주소 옵션을 지원하지 않습니다.가상 템플릿 인터페이스는 DSL 환경에 처음 구현되었습니다.현재 다이얼러 인터페이스는 DSL CPE 측에서 권장되는 컨피그레이션입니다.

IPSec과 다이얼러 인터페이스를 구성할 때 두 가지 문제가 발견되었습니다.

- Cisco 버그 ID CSCdu30070(등록된 고객만 해당) —DSL을 통한 소프트웨어 전용 IPSec:DSL 다이얼러 인터페이스의 입력 대기열 연결
- Cisco 버그 ID CSCdu30335(등록된 고객만 해당) —DSL을 통한 하드웨어 기반 IPSec:다이얼러 인터페이스의 입력 대기열 연결

이 두 가지 문제를 해결하는 현재 방법은 컨피그레이션에 설명된 대로 가상 템플릿 인터페이스를 사용하여 DSL CPE를 구성하는 것입니다.

이러한 두 문제에 대한 수정 사항은 Cisco IOS Software 릴리스 12.2(4)T에 대해 계획되어 있습니다.이 릴리스 후에는 다이얼러 인터페이스 구성을 다른 옵션으로 표시하기 위해 이 문서의 업데이트된 버전이 게시됩니다.

다음을 확인합니다.

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 데 사용할 수 있는 정보를 제공합니다.

여러 **show** 명령을 사용하여 피어 간에 IPSec 세션이 설정되었는지 확인할 수 있습니다.이 명령은 IPSec 피어(이 경우 Cisco 2600 및 3600 시리즈)에서만 필요합니다.

일부 **show 명령은** 출력 인터프리터 툴 에서 지원되는데(등록된 고객만), 이 툴을 사용하면 **show 명령 출력의 분석 결과를 볼 수 있습니다.**

- **show crypto engine connections active(암호화 엔진 연결 활성** 표시) - 각 2단계 SA가 빌드되고 전송된 트래픽의 양을 표시합니다.
- **show crypto ipsec sa** - 피어 간에 구축된 IPSec SA를 표시합니다.

다음은 show crypto **engine connections active** 명령의 샘플 명령 출력입니다.

```
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
```

show crypto ipsec sa 명령에 대한 샘플 명령 **출력입니다**.

```
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:
```

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

debug `atm events` 명령 보고하는 "Modem state = 0x8" 메시지는 일반적으로 WIC1-ADSL이 연결된 DSLAM에서 Carrier Detect를 수신할 수 없음을 의미합니다.이 경우 고객은 RJ11 커넥터와 관련하여 DSL 신호가 중간 2개의 와이어에 프로비저닝되었는지 확인해야 합니다.일부 Telcos는 대신 외부 두 핀에 DSL 신호를 프로비저닝합니다.

문제 해결 명령

일부 **show 명령은** 출력 인터프리터 툴 에서 지원되는데(등록된 고객만), 이 툴을 사용하면 **show 명령 출력의 분석 결과를 볼 수 있습니다.**

참고: debug 명령을 실행하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

주의: 라이브 네트워크에서 디버깅을 실행하지 마십시오.표시되는 정보 볼륨은 데이터 플로우와 CPUHOG 메시지가 발급되지 않는 지점으로 라우터를 오버로드할 수 있습니다.

- **debug crypto IPSec** - IPSec 이벤트를 표시합니다.
- **debug crypto Isakmp** - IKE 이벤트에 대한 메시지를 표시합니다.

요약

ADSL 연결을 통해 IPSec을 구현하면 지사와 중앙 사이트 간에 안전하고 안정적인 네트워크 연결이 가능합니다.ADSL-WIC 및 하드웨어 암호화 모듈과 함께 Cisco 2600/3600 Series를 사용하면 ADSL 및 IPSec을 단일 라우터 솔루션에서 구현할 수 있으므로 고객에게 더 낮은 소유 비용을 제공합니다.이 문서에 나와 있는 구성 및 주의 사항은 이러한 유형의 연결을 설정하는 기본 지침으로 사용해야 합니다.

관련 정보

- IPSec(IP Security) 암호화 소개
- Cisco 2600 Series 라우터
- 가상 사설 네트워크
- DSL 및 LRE 기술 지원
- 범용 게이트웨이 제품 지원
- 전화 접속 및 액세스 기술 지원
- Technical Support - Cisco Systems