링크 다중화를 통한 가상 사설망의 고가용성 및 부하 분산 기법

권 진 백*

요 약

VPN(Virtual Private Network)과 DSL, 케이블과 같은 다이얼업 접속의 조합은 저렴한 비용으로 임대라인 기반의 사설망의 대안이 되고 있다. VPN 장비의 고가용성(High Availability, HA)에 대한 기업의 요구가 증대되고 있다. 본 논문에서 VPN 게이트웨이에서 링크 이중화를 통한 액티브-액티브 방식을 이용해 네트웍 접근성의 고가용성과 네트웍 부하 분산 기법을 제안한다. 네트웍 링크의 고가용성/부하분산은 외부 내트웍 접근을 독립적인 두 개의 라인으로 이중화하는 것으로 달성할 수 있다. 이것은 둘 중 하나의 링크에 문제가 발생하더라도 내부 사용자에게 지속적인 네트웍 접근을 제공할 수 있다. 뿐만 아니라, 네트웍 부하를 두 개의 라인으로 분산시킴으로써 두 배에 가까운 네트웍 대역폭을 제공할 수 있다. 네트웍 링크의 부하 분배를 위해 정적인 알고리즘과 동적인 알고리즘을 제안한다.

High Availability and Load Balancing for Virtual Private Networks by Multiple Links

Jin Baek Kwon*

ABSTRACT

A combination of VPNs and dial-up access, such as DSL and Cable, usually provides the cost-effective solution as the substitution of private networks on high-cost leased line. The business demand for high availability has increased with VPN spreading. This paper presents the schemes for a high availability of network access and a load balancing of network traffic in VPN gateways by using multiple links or multihoming capability based on active-active approach. The high availability and load balancing of network links can be achieved by duplicating external network access into multiple independent links. This can provide a continuous network connection to internal users even if one of the links is failed. Moreover, it can provide twice network bandwidth by distributing the traffic into the links. Static and dynamic algorithms are proposed as the load balancing algorithms.

Key words : Virtual Private Network, High Availability

* 선문대학교 컴퓨터공학부

1. 서 론

VPN(Virtual Private Network)과 같은 네트워킹 장비의 고가용성(High Availability, HA)에 대한 기업의 요구가 증대되고 있다. 기업들은 네트웍 서비스 제공에 의존하고 있어, 장비의 다운 시간은 비용 손실은 물론 기업 이미지에 타격을 주게 된다. 장애가 없는(faultless) 완벽한 장비를 기대하기는 어렵기 때문에, 단일 장비로는 고가용성을 제공하기 불가능하다. 따라서, 장비의 신뢰성은 구성 장치의 다중화를 통해 제공할 필요가 있다. 하나의 장치만을 사용하고 나머지를 백업으로 두는 방식으로도 HA를 구현할 수 있지만, 이것은 다중화에 의한 성능 배가의 이점을 누리지 못한다. 따라서, 중복된 모든 장치를 사용해 부하를 분산(Load Balancing, LB)시키는 방식이 바람직하다. 최근의 네트웍 장비들은 세션의 상태를 유지하는 추세이므로, 중복된 장치 사이에 부하를 분산시키는 일은 많은 문제를 내포한다. 부하 분산은 기존의 패킷 포워딩 또는 라우팅에 의해 가능하지만, 터널링, 암호화, 패킷 필터링, 암호화, 인증과 같은 상태를 유지해야 하는 작업은 투명한 다중화가 매우 어렵다.

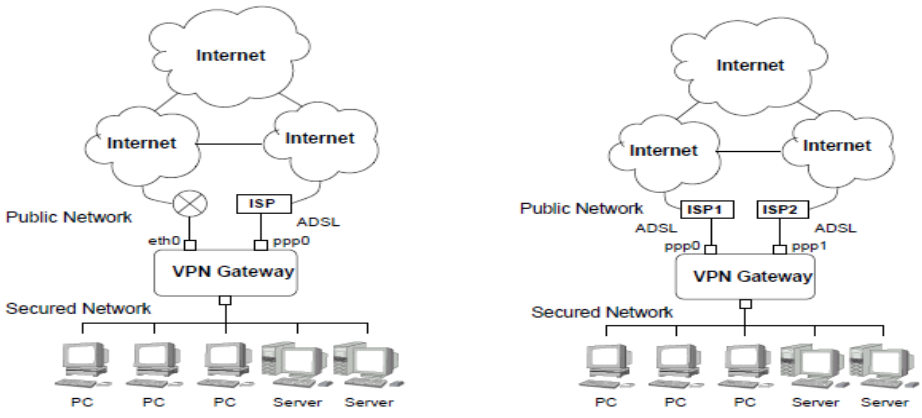
장치 다중화는 현재의 네트웍 환경에서 필수적인 기능들 중의 하나이다. VPN 게이트웨이 장비는 네트웍 내의 트래픽을 위해 충분하고 확장가능한 보안 서비스를 제공할 수 있어야 하고, 많은 수의 터널을 유지할 수 있어야 할 뿐 아니라, 높은 수준의 신뢰성을 제공해야 한다. 부하 분배와 고가용성은 다중화의 중요한 목적이다. 부하 분배의 목표가 성능향상이라면, 고가용성의 목표는 신뢰성(reliability)이다. 서비스을 이용할 수 없는 시간을 줄이는 것이 HA이다. 좀 더 구체적으로, 네트웍 장비의 경우 “가용하다”라는 것은 그 네트웍 장비를 통해 네트웍을정상적으로 접근할 수 있다라는 의미이다. 평상시 주장비(primary)만 서비스를 하고 다른 장비는 백업(backup)으로서 대기하다가 주장비가 고장났을 때 주장비의 역할을 대신하는 방법을 액티브-스탠드바이(active-standby) 방식이라고 한다. 하지만 이 방법은 LB등을 적용할 수 없어 자원 활용면에서 좋지 않다. 따라서, LB와 HA 동시에 적용하는 액티브-액티브(active-active) 방식이 더 바람직하다.

본 논문에서 링크 이중화를 통한 액티브-액티브 방식의 HA/LB를 제안한다. 즉, 외부 네트웍 인터페이스의 이중화를 이용한 네트웍 접근성의 HA와 네트웍 부하의 LB 기법을 제안한다. 네트웍 링크의 HA/LB는 외부 내트웍 접근을 독립적인 두 개의 라인으로 이중화하는 것으로 달성할 수 있다. 이것은 둘 중 하나의 링크에 문제가 발생하더라도 내부 사용자에게 지속적인 네트웍 접근을 제공할 수 있다. 뿐만 아니라, 네트웍 부하를 두 개의 라인으로 분산시킴으로써 두 배에 가까운 네트웍 대역폭을 제공할 수 있다. 네트웍 라인의 부하 분배를 위해 정적(static)인 알고리즘과 동적(dynamic)인 알고리즘을 제공한다.

본 논문의 나머지 부분은 이 두 가지 HA/LB를 더 상세히 다룰 것이다. 제안된 VPN 게이트웨이는 IETF에서 규정하는 VPN의 표준인 IPsec을 따라 구현되었다[1-5]. IPsec에서는 인터넷 상에서의 비밀성을 위해 터널 모드와 트랜스포트 모드를 규정하고 있지만, 터널 모드가 더 일반적으로 널리 쓰이므로 이 논문에서는 터널 모드만 다루기로 한다. 하지만, 이 모든 기술들은 트랜스포트 모드에도 동일하게 적용된다.

2. 링크 이중화에 의한 HA/LB 기법

이 절에서 외부 네트웍 링크의 이중화를 이용한 네트웍 접근성의 고가용성과 네트웍 부하 분배를 이용한 네트웍 성능 향상 방법을 소개한다. (그림 1)은 본 논문에서 제안하는 VPN 네트웍 링크 이중화 구성을 보여준다. (그림 1)의 (a)는 전용선과 ADSL을, (b)는 두 개의 ADSL을 통해 외부 네트웍에 접근하는 구성을 보여준다.



(a) LAN-ADSL (b) ADSL-ADSL

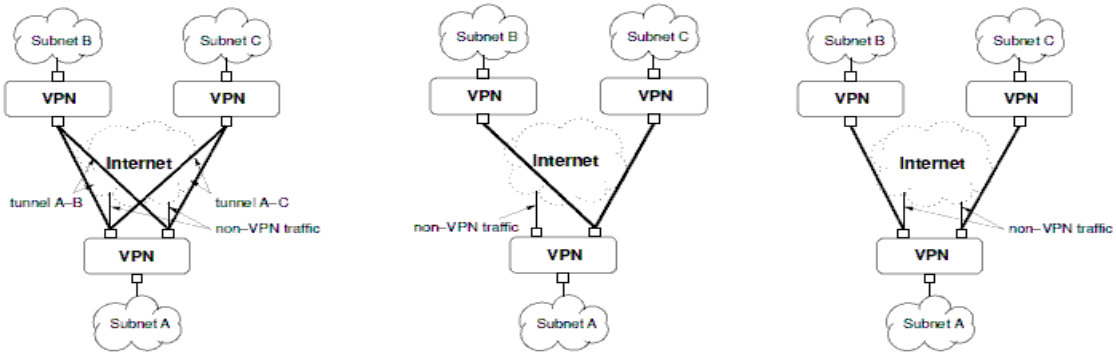
(그림 1) 링크 이중화

2.1 동비용 다중 경로(Equal Cost Multipath : ECM)

정상적인 경우, 라우팅 테이블은 주어진 패킷에 대해 항상 동일한 단일 동작을 하도록 정해져 있다. 즉, 패킷은 라우팅 테이블에서 매칭(matching)되는 엔트리(entry)에 정해진 인터페이스를 통해, 그 인터페이스에 해당하는 목적지로 보내진다(같은 패킷에 대해 항상 같은 인터페이스를 통해 보내진다). 하지만, 동비용 다중경로(equal cost multipath : ECM, RFC1583)[4] 기법을 사용하면, 라우팅 테이블에 특정 목적지에 대해 여러 개의 다른 경로(인터페이스)를 지정할 수 있다. 이 때, 각 경로는 동등하게 평가되고, 출발지(source)/목적지(destnation) 쌍에 대해 경로가 결정된다. 예를 들어, 출발지 a에서 목적지 b로 가는 패킷이 인터페이스 1로 라우팅이 되면, 다음 출발지 a에서 목적지 c로의 패킷은 인터페이스 2로 라우팅이 된다. 즉, 라운드-로빈(round-robin) 방식으로 라우팅이 된다.

2.2 부하 분배 알고리즘

(그림 2)는 세 가지의 부하 분배 알고리즘을 보여준다. VPN 장비가 VPN 패킷(터널을 통과하는 패킷)만 다루는 것이 아니라 non-VPN 패킷(일반 패킷)도 고려해야 한다. 그림에서 (a)는 모든 터널을 두 개로 중복시켜 각각의 인터페이스에 바인딩시키고, VPN 패킷과 non-VPN 패킷 모두에 대해 ECM 기법을 적용시켜 양 인터페이스로 분배시키는 방법이다. (b)는 터널을 하나의 인터페이스에 전담시키고, non-VPN 패킷은 다른 인터페이스로만 보내는 방법이다. 즉, VPN 패킷과 non-VPN 패킷이 다른 인터페이스로 완전히 분리시키는 것이다. 이 때, ECM은 사용되지 않는다. (c)는 (a)와 (b)를 결합한 형태로, 터널의 중복없이 터널 별로 다른 인터페이스에 바인딩시키고, VPN 패킷에는 ECM 기법을 적용시키지 않고, non-VPN 패킷에만 ECM을 적용시키는 방법이다. (a) 방법이 부하 분배면에서 가장 이상적이다. 왜냐하면, 터널 별로 네트웍 부하가 다르기 때문에 각 터널 내의 부하를 분배시키는 것이 터널별 부하 차이를 극복할 수 있기 때문이다. 하지만, 현재 IPsec 표준에 따르는 시스템에서는 이러한 구조는 불가능하다. 이유는 아래와 같다. IPsec에서는 SA(Security Association)을 정의하는데[1], 이 SA에는 그 터널에 사용할 인



(a) 이상적인 알고리즘 (b) 정적 알고리즘 (c) 동적 알고리즘

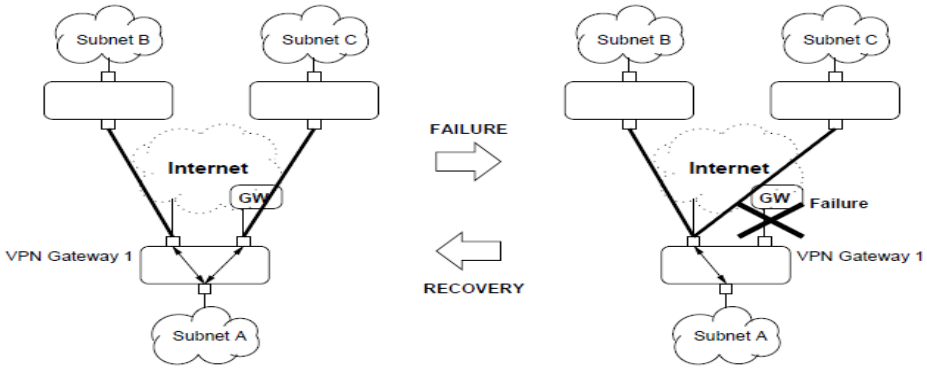
(그림 3) 부하 분배 알고리즘

증 알고리즘, 암호화 알고리즘 등이 규정된다. 하나의 VPN 터널의 대상은 종단 서브넷 또는 호스트로 정의되는데, 이 연결은 SA들의 그룹으로 규정된다. 여기서 주목해야 할 것은 하나의 연결에 오직 하나의 SA 그룹이 배정되어야 한다는 것이다. 따라서, 같은 서브넷 쌍에 대해 두 개 이상의 터널을 정의할 수 없다는 것이다. 예를 들면, (그림 2)(a)에서 서브넷 A와 서브넷 B에 대해 오직 한개의 터널만이 정의되어야 한다. 즉, A에 있는 호스트에서 B에 있는 호스트로 보낸 패킷이 통과하는 터널은 오직 한 개이어야 한다는 것이다. 여러 개의 터널이 가능하려면 실행시 터널을 선택하는 방법이 있어야 하고, 상대쪽 VPN 장비에서도 그 패킷이 통과한 터널이 무엇인지 알고 있어야 한다. 현재 IPsec 상에서 이것은 불가능하므로, 알고리즘 (a)는 구현이 불가능하다.

제안한 VPN에서는 알고리즘 (b)와 알고리즘 (c)를 제공하는데, 전자를 정적(static) 알고리즘, 후자를 동적(dynamic) 알고리즘이라고 한다. 정적 알고리즘은 부하 분배 측면에서 동적 알고리즘보다 못하지만, non-VPN 트래픽이 상대적으로 많을 때 VPN 트래픽의 QoS(Quality of Service)를 어느 정도 보장해 줄 수 있다. 다시 말하면, 정적 알고리즘은 VPN 트래픽의 QoS 측면에서 좋고, 동적 알고리즘은 전체 부하의 균등면에서 좋다. 뿐만 아니라, 동적 알고리즘은 터널의 개수가 여러 개라면 확률적으로 터널의 부하 차이가 상쇄되므로 어느정도 이상적인 알고리즘((그림 2)(a))에 근접할 수 있다.

2.3 고가용성(High Availability : HA)

HA 지원에서 가장 중요하면서 기본적인 문제는 “장애 발생을 어떻게 감지할 것인가?”이다. 링크 이중화의 경우, 링크 장애를 감지하는 것이 가장 먼저 해결해야 할 문제인 것이다. 제안한 VPN은 각 인터페이스의 게이트웨이로 ICMP 패킷을 주기적으로 보내서 타임아웃(timeout) 전에 응답이 오는지를 체크하는 방법을 사용한다((그림 3) 참조). 타임아웃이 지정 회수를 초과하게 되면, 그 링크에 장애가 있는 것으로 판단하고 모든 트래픽을 다른 인터페이스로 라우팅되도록 라우팅 테이블을 수정한다. 게이트웨이로 ICMP를 주기적으로 보내는 일은 장애가 감지된 후에도 계속된다. 이는 링크의 복구를 감지하기 위함이다. 고장난 링크의 게이트웨이에서 ICMP 응답이 오기 시작하면 링크 복구로 판단하



(그림 5) 링크 고장/복구시 동작(동적 LB)

고 원래의 라우팅 테이블로 복귀시킨다.

결함 발생 및 복구시, non-VPN 패킷에 대해서는 라우팅 테이블만 수정해주면 되지만, VPN 패킷에 대해서는 그렇게 간단하지 않다. 고장난 링크의 인터페이스를 통해 VPN 터널이 존재하고 있었다면, 이 터널들을 해제하고 정상 링크의 인터페이스로 터널들을 재생성 해주어야 하기 때문이다. 또한, 링크 복구시 터널과 라우팅 테이블을 정상 상태로의 복귀 및 재생성시켜 주어야 한다. 타임아웃 값을 t, 타임아웃 회수를 n, 터널 재생성 시간과 라우팅 테이블 수정등 추가시간을 e라 할 때, 결함시 특정 연결이 마비되는 시간 T는

$$T = t \cdot (n+1) + e$$

된다. n에 1을 더하는 이유는 ICMP 응답을 받은 직후에 결함이 발생했다면, t시간이 추가되기 때문이다. 예를 들어, 타임아웃 값이 5초, 회수가 2번, 추가시간이 2초라면 $5 \times 3 + 2 = 17$초가 된다.

3. 토의 및 관련 연구

본 논문에서는 링크 이중화는 네트웍 링크의 LB와 HA를 다루었다. VPN 장비 자체를 다중화해서 VPN 처리(암복호화 및 인증)의 부하 분배와 VPN 장비의 HA를 소개한다. VPN 처리는 많은 CPU 자원을 요구하기 때문에, 장비를 다중화하고 CPU 부하의 분산함으로써 전체 VPN 처리 성능을 높일 수 있다. 또한, 네트웍 링크와 마찬가지로 네트웍 장비 자체도 여러 가지 이유(하드웨어적 고장, 전원 불안정, 시스템 점검 등등)로 패킷 처리를 하지 못할 수 있다. 이때도 링크 장애와 같이 사용자에게 VPN등 네트웍 접근을 제공할 수 없게 된다. 이런 네트웍 불능 상태는 금융망, 유통망 등 대부분의 기업망에서 치명적이다. 따라서, VPN 장비의 다중화로 HA를 제공하는 것이 필수적으로 요구되고 있다. 클라이언트-서버 협력식과 서버 주도식이 그것이다. 전자는 클라이언트가 LB/HA에 관여하는 방법으로 응용 수준에서 구현가능하고, 후자는 클라이언트에 완전히 투명한 방식으로 커널 수준에서 구현되어야 한다.

4. 결 론

네트웍 장비는 여러 사용자가 공동으로 사용하는 장비이므로 HA 기능이 필수적이다. HA는 보

통 장비나 구성요소의 다중화로 구현되는데, 다중화를 더 효율적으로 이용하기 위해 HA와 함께 LB 기능도 함께 제공하는 것이 바람직하다. 본 논문에서 액티브-액티브 방식의 HA/LB 기법을 제안한다. 외부 네트웍 인터페이스의 이중화를 이용한 네트웍 접근성의 HA와 네트웍 부하의 LB를 제안하였고, 이 라인 이중화는 LAN-ADSL, ADSL-ADSL, ADSL-PSTN 방식을 지원할 수 있다.

참 고 문 헌

[1] S. Kent and R. Atkinson, “Security Architecture for the Internet Protocol”, RFC 2401, 1998.

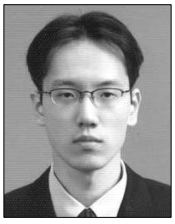
[2] Alcatel, “Understanding the IPsec Protocol Suite”, Technical Paper, March 2000, http://www.cid.alcatel.com.

[3] D. Harkins and D. Carrel, “The Internet Key Exchange (IKE)”, RFC 2409, 1998.

[4] D. Harkins and D. Carrel, “IP Authentication Header”, RFC 2402, 1998.

[5] S. Kent and R. Atkinson, “IP Encapsulating Security Payload”, RFC 2406, 1998.

[6] J. Moy, “OSPF version 2”, RFC 1583, 1994.



권 진 백

1998년 한국외국어대학교 정보통계학과(이학사)

2000년 서울대학교 전산과학과(이학석사)

2003년 서울대학교 컴퓨터공학부(공학박사)

2003년~현재 선문대학교 컴퓨터공학부 조교수