論文2001-38TC-11-2

SCG(Secure Communication Group)을 이용한 계층적 VPN(Virtual Private Network) 구성 및 특성

(Hierarchical VPN Configuration Method using SCG(Secure Communication Group) and Its Characteristics)

朴 贊 祐 *, 韓 致 文 *

(Chan-Woo Park and Chimoon Han)

요 약

인터넷을 이용한 대부분의 VPN(Virtual Private Network)은 기업 데이터만을 보호하는 형태로 구성되어 있다. 그러므로 다양한 형태의 VPN 구성이 필요하다. 최근에 SCG(Secure Communication Group) 개념을 이용하여 VPN을 구성하는 방법이 연구되고 있다. 본 논문에서는 SCG 구성 방법인 Path-definition 방식과 Area-definition 방식의 문제점을 분석하고, 인트라넷 VPN 환경에서 SCG 개념을 사용한 VPN 중 적용 가능한 여러 형태의 VPN 모델을 검토한다. 그리고 인터넷에 Area-definition 방식을 적용하고 SCG number를 이용한 계층적 VPN 구성 방법을 제안한다. 제안한 방식의 특성을 각 entity가 관리해야 할 키 수 및 인증 회수에 대해 정량적으로 분석하고, 본 방식이 유효함을 나타낸다.

Abstract

Currently most of VPNs within internet has only capability to protect cooperate data. Recently, various types of VPNs are being studied based on the concept of SCG(Secure Communication Group). This paper analyses the problems of path-definition method and area-definition method of VPNs using SCG technology, and discusses the possible models among VPNs using SCG technology. This paper proposes the hierarchal VPN configuration method using SCG number and internet based area-definition method, and analyze the characteristics of the proposed VPN model on the point of the authentication frequency and the number of managements keys.

I. 서 론

대부분의 기업이나 공공 기관은 통신 사업자로부터 전용회선을 임대하여 본사와 지사를 연결함으로써 지역적인 제한 없이 업무를 수행하는 형태로 사설망을 확장 시켜 왔다. 이렇게 구축된 사설망은 네트워크 장비와 소프트웨어의 초기 투자비용이 많이 들 뿐만 아니라 회선 요금도 높다. 이와 같이 고비용의 문제점을 해결하기 위한 방안으로 인터넷을 이용한 VPN(Virtual Private Network)이 연구되고 있다. 한 방법으로 VPN은 전용 임대회선 대신에 인터넷을 이용하고 있다. VPN에 적절한 암호기술을 이용하면, 한 조직의 내부 사용자들이 사내와 사외에서 서로 안전하게 통신할 수 있는 채널을 형성해 주며 또한 필요에 따라 접근 제어 기능을 제공해 줄 수 있다. 즉, 논리적 의미로 VPN은

* 正會員, 韓國外國語大學校 電子情報工學部
(School of Electronics and Information Engineering, Hankuk University of Foreign Studies)
接受日字:2000年7月15日, 수정완료일:2001年10月22日

CUG(Closed User Group)으로 간주 할 수 있다.

현재 구축되어 있는 VPN을 분류하면 인트라넷 VPN, Remote Access VPN, 엑스트라넷 VPN의 세가지 형태로 나눌 수 있다. 이러한 VPN은 모두 공중망에서의 안정성만을 보장하는 방식이다. 그러나 기업 내부에서는 다양한 종류의 데이터가 존재한다. FBI나 CSI(Computer Security Institute)의 공동 조사에 따르면 실제로 보안 침해의 반 이상은 내부에서 일어난다고 한다. 따라서 다양한 종류의 데이터를 데이터 등급에 맞게 보호 할 수 있는 VPN 구성이 필요하다. 즉, 기업 내부에서도 부서별로 소규모의 논리적인 VPN을 구성할 수 있는 개념이 요구된다[1~3].

최근 암호를 기반으로 한 SCG(Secure Communication Group)의 개념을 이용하여 다양한 형태의 VPN 구성 방법이 연구되고 있다[4,5,7]. SCG 구성 방법은 키의 분배 형태에 Path-definition 방식과 Area-definition 방식으로 나눌 수 있다. IPSec(IP Security Protocol) & IKE(Internet Key Exchange)로 구성한 Path-definition 방식은 강력한 보안과 적용 범위가 넓지만 관리를 위한 트래픽의 양이 많고, GSP(Group Search Protocol)을 이용한 Area-definition 방식은 인트라넷 내부에 적용하기에 적합한 방식이지만[5,7] 인터넷을 통한 VPN 구성에는 적합하지 않다. 따라서 본 논문에서는 다양한 형태의 VPN을 구성하기 위하여 인트라넷 환경에서 SCG의 개념을 도입한다. SCG을 구성하기 위해 Path-definition 방식과 Area-definition 방식의 특성과 문제점을 분석하고, SCG number를 도입한 계층적 VPN 구성 방법을 제안한다.

본 논문은 서론에 이어 Ⅱ에서는 SCG 정의 및 SCG 구성 방법에 대해서 설명보고, Ⅲ에서는 Area-definition 방식이 인터넷 환경에 적용 가능한 VPN을 SCG number를 이용하여 구성하는 방법을 검토한다. Ⅳ에서는 인트라넷 환경에서 SCG number를 이용한 계층적 VPN 구성하는 방법을 제안하고 그 특성을 분석한다. Ⅴ에서 결론을 맺는다.

Ⅱ. SCG 정의 및 SCG 구성 방법

1. SCG(Secure Communication Group)의 정의[4]

모든 통신 경로마다 Full Mesh 형태로 암호화를 위한 키를 가지고 있거나 같은 암호키를 공유하고 있는 그룹을 SCG(Secure Communication Group)이라 한다.

그림 1은 Path-definition 방식으로 구성한 SCG이다. 여기서 CE(Communication Entity)는 암호화 장치가 있거나 암호화를 위한 소프트웨어가 실장 되어 있는 단말 혹은 서브 네트워크를 의미한다. MGE(Management Entity)는 각 CE를 인증하고, 암호키 관리 등의 일을 수행하는 서버를 의미한다. 동작 원리는 MGE에서 CE의 리스트를 가지고 모든 통신 경로상의 CE에 대응하는 키를 분배한다. 각 CE는 대응하는 CE와 같은 쌍의 키를 가지고 암호 통신을 함으로써 하나의 SCG를 구성하게 된다.

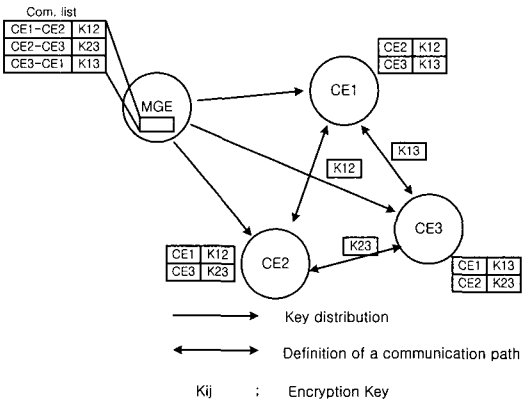

그림 1. Path-definition 기반 SCG 구성
Fig. 1. Path-definition based SCG configuration method.

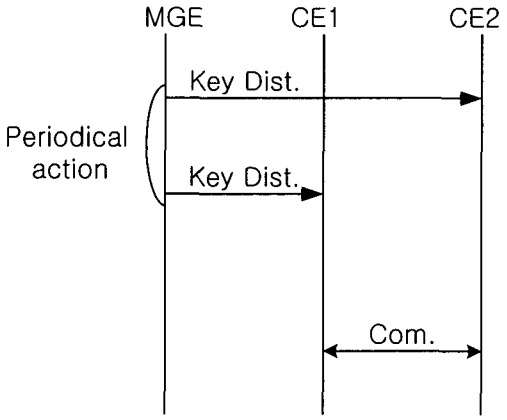

그림 2. 주기적 키 분배 방식
Fig. 2. Periodical key distribution method.

MGE에서 SCG의 각 CE에 키를 분배하는 방법은 주기적으로 키를 분배하는 방식과 요구가 있을 때 키를

분배하는 방법이 있다. 그림 2는 주기적으로 키를 분배하는 방식이다. 이는 시스템이 대규모일 경우에 키의 수도 선형적으로 증가하기 때문에 시스템 트래픽이 증가하는 단점을 가지고 있다.

그림 3은 요구가 있을 때 키를 분배하는 방식이다. 이는 키를 관리해야 하는 트래픽 면에서 장점을 가질 수 있으나, 키를 분배하는 프로세스 초기화 과정에서 지연과 이로 인해 다른 시스템의 효율에 나쁜 영향을 준다. 인증은 각 MGE와 CE 간, 각 CE 간에 요구가 있을 때마다 인증 과정이 수행되어야 한다.

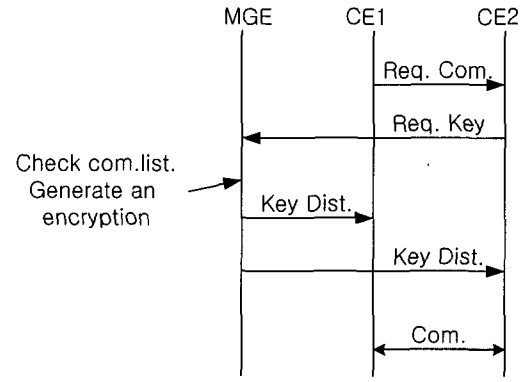

그림 3. 요구형 키 분배 방식
Fig. 3. On-demand key distribution method.

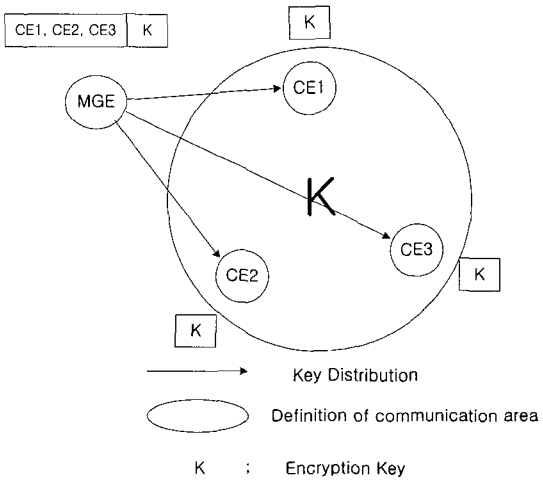

그림 4. Area-definition 기반 SCG 구성
Fig. 4. Area-definition based SCG configuration method.

그림 4는 Area-definition 방식으로 구성한 SCG이다. Path-definition과 달리 하나의 Area를 정의하여 동일한 키를 분배하는 방식이다. 즉 같은 키를 공유하고 있는 CE의 집합이 하나의 SCG가 된다. 즉 CE1, CE2, CE3는 모두 동일한 암호키 K를 사용하여 통신을 하게 된다. 이때 각각 키를 분배하는 방식은 주기적으로 키를 분배하는 방식과 요구가 있을 때 키를 분배하는 방식을 사용할 수 있다.

그림 5는 주기적으로 키를 분배하는 방식이다. Area-definition 방식에서는 CE의 수가 증가하더라도 키의 수가 선형적으로 증가하지는 않기 때문에 주기적 키 분배 방식을 주로 사용한다. 키를 분배하기 전에 MGE와 CE 사이에 인증이 필요하다. KEYDIST는 인증 헤더와 암호화된 키를 포함한다. 주기적 키 분배 방식에서 문제가 될 수 있는 부분은 예전 키와 새로운 키가 동시에 존재하는 경우이다. 이 문제는 STOP/RESTART 명령으로 CE에 키가 두개 이상 존재하는 문제점을 해결 할 수 있다.

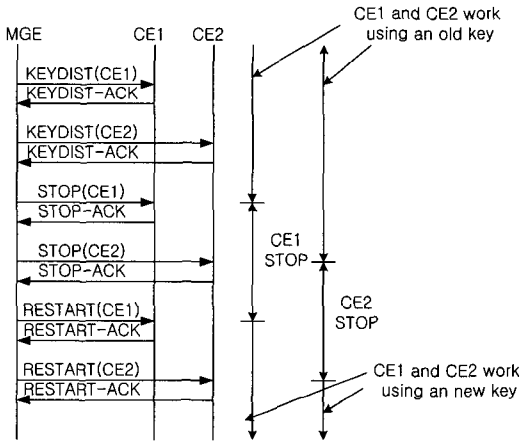

그림 5. 주기적 키 분배 방식
Fig. 5. Periodical key distribution method.

2. SCG(Secure Communication Group) 구성 방법

그림 6은 IPSec & IKE를 이용하여 SCG를 구성하는 방법을 나타낸 것이다[6]. 초기화 과정으로 MS에서는 각 CE에 공개키를 분배하고, 이는 통신 경로상의 각 peer CE(Communication Entity) 사이의 인증에 사용된다. 그리고, SPD(Security Policy Database)가 각 EE(Encryption Entity)에 키를 분배된다. SPD는 각 EE의 동작을 정의한 파라미터로 예를 들어, 이 경우는 CE1은 CE2, CE3와 통신하도록 정의되었다. 통신이 시작되면 각 peer CE는 SA(Security Association)를 설정한다. SA process에서는 통신 경로상의 peer CE와 통신이 허가되면, 공개키를 사용하여 서로 인증절차를

거치고 암호키를 생성하여 공유하게 된다. SA 생성 후 IP Security Format으로 통신을 한다. 시스템이 완벽하게 동작을 하려면 SPD가 매우 커야 한다. 이는 SA의 초기 설정시 지연과 같은 성능의 저하와 패킷의 길이가 변화에 따르는 효율 저하를 가져올 수 있다.

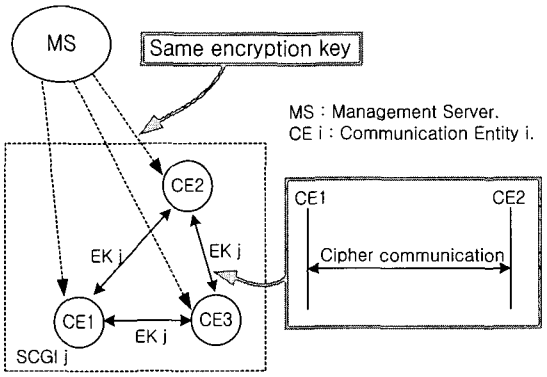

그림 7. GSP를 이용한 SCG 구성
Fig. 7. SCG configuration using GSP.

3. 비교 및 분석

Path-definition 방식에서 SCG 구성 정보는 MS (Management Server)에서 SCG의 정의와 IP 주소에 관련된 정보로부터 계산된다. 이 계산 값과 SCG 구성 정보의 집합은 MS로부터 초기값으로 다운로드 된다. 이 방법은 물리적인 구성상의 변화가 일어날 때 마다 매번 IP 주소와 관계된 정보를 등록 해야 하고 새로운 파라미터를 생성하여 다운로드 해야 한다. 따라서 관리해야 할 트래픽의 양이 많다. 또한 각 CE마다 인증과정을 수행하기 때문에 지연이 크다.

Area-definition 방식은 GSP를 이용하여 인트라넷 내부에서 SCG를 구성할 수 있다. 이 방식은 인트라넷 내부에서는 키의 수와 인증 수행으로 인한 지연이 IPSec & IKE로 구현한 SCG보다 유리하다. 하지만 이 방식은 IP에 독립적으로 동작한다. 따라서 공중망(인터넷)을 통한 다른 인트라넷에 사용이 불가능하다.

표 1은 IPSec & IKE와 GSP로 구성한 SCG을 비교한 것을 요약하여 나타냈다. IPSec & IKE는 관리면에서 복잡한 등록절차로 인하여 성능 저하요인이 많은 반면에 GSP는 성능 저하 요인이 적다. 따라서 물리적 인트라넷 내부에서는 GSP를 이용하여 SCG를 구성하는 것이 바람직한 것으로 보인다. 하지만 GPS는 IP에 독립적으로 동작하므로 인터넷을 통하여 적용하는 것은 불가능하다. 그러므로 키의 수와 인증으로 인한 지연을 줄일 수 있는 Area-definition 방식을 인터넷에 적용할 수 없다. 따라서 Area-definition 방식을 인터넷에 적용시킬 수 있는 방법이 요구된다. 이는 GSP를 통하여 SCG를 구성하고 이를 통해 얻어지는 SCG number를 각 인트라넷에 있는 MS 간에 공유 시킴으로써 구성이 가능하다.

표 1. IPSec & IKE와 GSP의 비교
Table 1. Compare IPSec & IKE with GSP.

	IPSec & IKE	GSP
Key 할당	Path-based	Area-based
Key 공유	요구가 있을 때	주기적
관리	복잡함 -등록 정보량 많음 -IP주소에 종속적 -Fixed system에 유용	단순함 -단순한 Parameters -IP주소에 독립적 -Location free
성능	성능저하요인 -IKE 협상 -Encapsulation -Encryption	성능저하요인 -Encryption
보안	엄격함	같은 SCG 내에서 키 도용이 가능
유용한 곳	Open network (Internet)	Close Network (Intranet)

Ⅲ. SCG number를 이용한 VPN 구성

인트라넷 내부의 SCG와 다른 인트라넷의 SCG간에 새로운 SCG 구성은 SCG number를 이용한 새로운 VPN 구성이다. 즉, 인트라넷 VPN에서 서로 다른 인트라넷에 있는 그룹을 연결하고자 하는 구조이다. 이는 인트라넷 내부에서는 GSP를 이용하여 Area-definition 방식으로 SCG를 구성하고, 다른 인트라넷의 CE와 SCG를 구성하고자 할 경우에는 SCG number 정보를 이용하여 구성하면 된다. 여기서 Management Server 사이에 SCG topology 정보의 공유와 새로운 SCG 구성 파라미터의 전달은 Path-definition 방식을 사용한다. SCG number를 이용하여 다른 인트라넷 상에 있는 SCG와 SCG를 구성하기 위한 동작 순서를 나타냈다 (여기서 init CE와 MS는 새로운 SCG를 구성하고자 요청하는 주체이고, target MS와 CE는 SCG를 구성하고자 하는 다른 인트라넷에 속한 것을 의미한다).

① 인트라넷 내부에서는 GSP를 이용하여 SCG를 구성
② CE는 자신이 속해있는 SCG number를 MS에 전송(인트라넷 내부이므로 안전함. 또는, 인트라넷 내부의 암호키를 이용하여 전송)
③ MGE는 인트라넷의 SCG구성 topology를 파악
④ 각 인트라넷에 속해있는 MS 사이에 SCG구성 topology 정보를 주고 받아 동기화 시킴(topology의 변화가 생길 때 변경하여 동기화를 유지함)
➡ 인트라넷 내부에서 SCG를 구성하는 과정(초기화 과정)
⑤ 다른 인트라넷에 있는 SCG와 새로운 SCG를 구성하고자 할 때 init CE가 SCG 구성 요청 메시지를 init MS에 전송
⑥ 요청 메시지를 수신한 init MS는 target MS에 의뢰함
⑦ target MS는 target SCG의 대표 CE에 요청메시지 송신
⑧ target SCG의 대표 CE는 수락 혹은 거부 메시지를 target MS에 송신
⑨ target MS에서 SCG구성을 위한 파라미터를 생성하여 송신
⑩ init MS와 target MS는 SCG 파라미터를 각 CE에 분배하고 SCG topology 정보를 변경 시킴
⑪ 새로운 Secure Communication Group이 생성됨

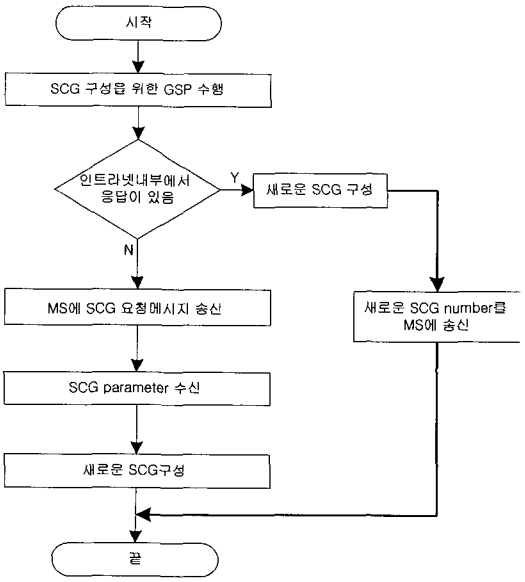

그림 8. init Communication Entity의 동작 절차
Fig. 8. Operation procedure of init communication entity.

그림 8은 init CE의 동작 절차이다. 초기화 과정을 거친 후 CE는 SCG를 구성하기 위하여 GSP 프로토콜을 수행하게 된다. 이때 인트라넷 내부에서 응답이 있으면 SCG를 구성한다. 인트라넷 내부에서 응답 메시지가 없으면 MS에 SCG 구성을 의뢰하는 메시지를 송신한 후 대기한다. MS로부터 SCG 구성을 위한 파라미터를 수신하면, 다른 인트라넷과 새로운 SCG를 구성하게 된다.

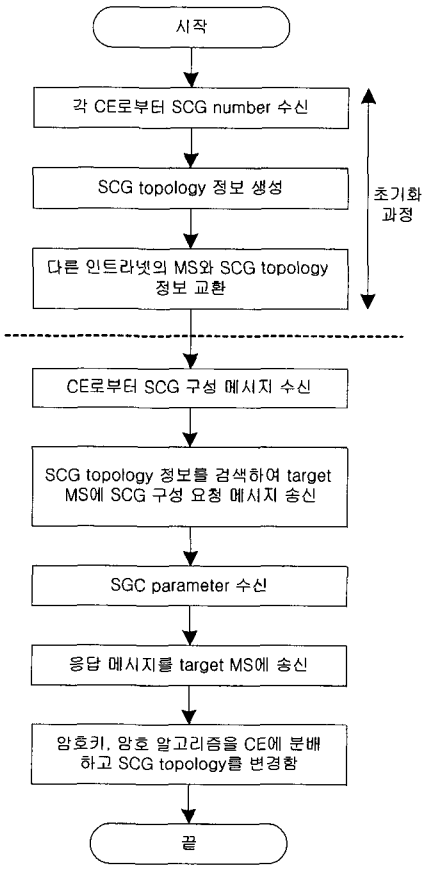

그림 9. init Management Server의 동작 절차
Fig. 9. Operation procedure of init management server.

그림 9는 init MS의 동작 절차이다. 초기화 과정에서 SCG 구성을 정의한 파라미터는 각 CE에 분배된다. 이후 GSP프로토콜을 이용하여 각 CE에서 SCG를 구성하고 이 SCG number를 MS에 전송한다. 따라서 MS는 SCG 구성을 위한 파라미터의 생성이나 계산과정 없이 SCG number를 수신하여 인트라넷 내부의 SCG 구성 형태 정보만을 가지게 된다.

SCG 구성 형태 정보는 다른 인트라넷의 MS와 동기화를 맞추어 전체 SCG 구성 정보를 가지게 된다. 구성 정보만을 공유하게 되므로, 전체 시스템 성능에 크게 영향을 미치지 않는다.

CE로부터 SCG 구성 메시지를 수신하면 SCG topology 정보를 검색하여 해당 인트라넷의 MS에 SCG 구성 메시지를 송신한다. 암호키와 알고리즘을 수신하면 target MS에 응답 메시지를 송신하고 CE에 암호키와 알고리즘을 분배한다. SCG가 구성된 것을 확인하고 구성 정보를 변경한다.

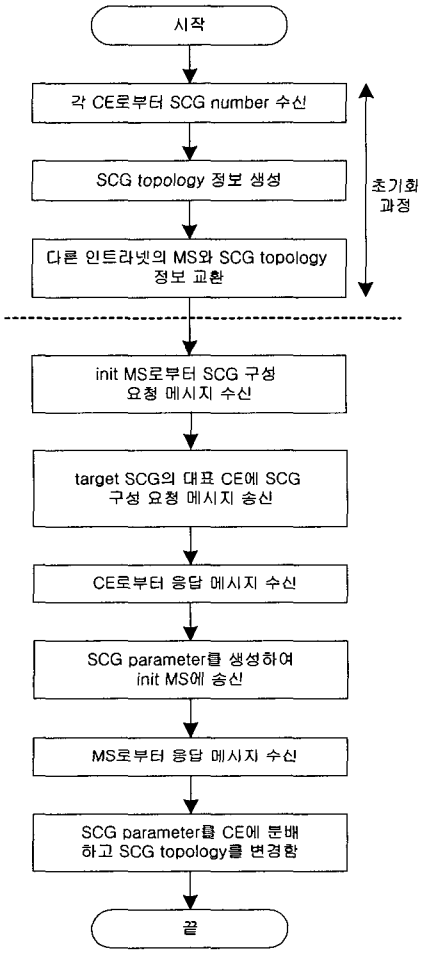

그림 10. target Management Server의 동작 절차
Fig. 10. Operation procedure of target management server.

그림 10은 target MS의 동작 절차이다. target MS는 초기화 과정으로 SCG의 구성 정보를 가지고 있다. init MS로부터 SCG 요청 메시지를 수신하면 SCG 구성 정보를 검색하여 해당 SCG의 대표 CE에 메시지를 송신한다. target CE로부터 메시지를 수신하면 target MS는 SCG를 구성하기 위한 파라미터를 생성하여 init MS에 송신한다. Init MS로부터 응답 메시지를 받은 후 target SCG의 각 CE에 SCG 구성 파라미터를 송신한다. 새로운 SCG 구성을 확인한 후 SCG 구성 정보를 변경한다.

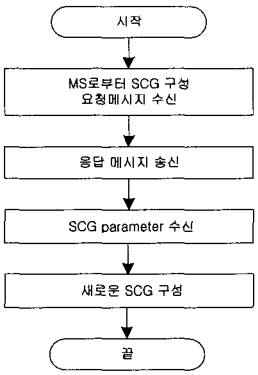

그림 11. target Communication Entity의 동작 절차
Fig. 11. Operation procedure of target communication entity.

그림 11은 target CE의 동작 절차이다. target CE는 MS로부터 SCG 구성 요청 메시지를 수신하면 target MS에 응답 메시지를 송신한다. 이후 SCG 구성을 위한 파라미터를 수신하고 새로운 SCG를 구성하게 된다.

Ⅳ. SCG 기반 계층적 VPN 구성 방법

본 장에서는 인트라넷 VPN에 한정 지어 검토하기로 한다. 그림 12는 SCG를 이용하여 계층별로 VPN을 구

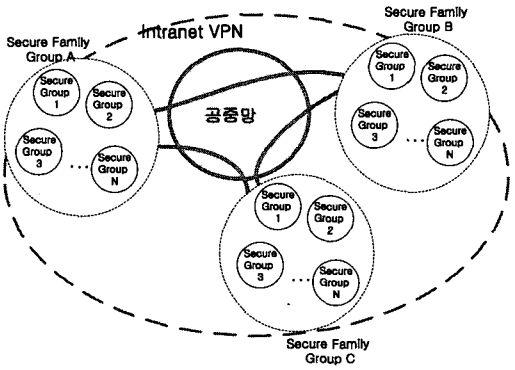

그림 12. 계층적 VPN 구성 방안
Fig. 12. Hybrid-VPN configuration method.

성한 개념도이다. VPN의 계층적 구성 방식으로 Secure Family Group(SFG) 단위(본사 혹은 지사 내부에 해당), Secure Group 단위(기업 내의 각 부서에 해당)와 Communication Entity 단위(단말 혹은 sub-network)로 구분한다. 이는 VPN 내부에 또 다시 SCG 개념을 적용한 소규모의 VPN을 구성한 개념이다.

1. 기존의 방식을 이용한 계층적 VPN 구성 방법

표 2는 그림 12에서 제시한 VPN 구조를 기본으로 구성 가능한 VPN 방식을 검토한 것이다. 표 2에서 알 수 있듯이 적용 가능한 모델은 4가지이다. SFG (물리적 인트라넷)의 내부에서는 Path-definition 방식과 Area-definition 방식을 모두 적용하여 SCG를 구성 할 수 있지만, Secure Family Group간(즉, 논리적 인트라넷)에는 Area-definition 방식을 적용할 수 없다. 여기서 Path-definition 방식은 IPSec&IKE를 이용하여 구성할 수 있고, Area-definition 방식은 GSP를 이용하여 구성할 수 있다.

표 2. 계층적 VPN 구성 방안
Table 2. Hierarchical VPN configuration method.

	Secure Group 내	Secure Group 간	Secure Family Group 간	적용 가능성
방식1	Path	Path	Path	○
방식2	Path	Path	Area	×
방식3	Path	Area	Path	○
방식4	Path	Path	Area	×
방식5	Area	Path	Path	○
방식6	Area	Area	Area	×
방식7	Area	Area	Path	○
방식8	Area	Path	Area	×

2. SCG number를 이용한 계층적 VPN 구성 방법 제안

SCG number를 이용하는 계층적 VPN 구성 방법을 제안한다. 제안하는 VPN은 인트라넷 내부에서는 GSP를 이용하여 SCG를 구성하고, 인터넷 환경에서는 IPSec & IKE를 사용하여 SCG를 구성하는 방식이다. 즉 SFG내에서는 GSP(Group Search Protocol) 프로토콜을 이용하여 Area-definition 방식으로 VPN을 구성하고, 다른 SFG의 SG와 새로운 SCG 구성은 MS(Management Server)에 암호 알고리즘과 키를 생성하여 각 CE(Communication Entity)에 분배하고, 이를 이용하여 새로운 SCG를 구성한다. 따라서 본 방식은 SFG간의 MS사이에는 Path-definition 방식이 적용되지만, CE 기반 암호키는 SCG당 하나만 관리하면 되므로 Area-definition 방식을 적용한 것과 같다. 인터넷 환경에서는 각 MS는 SCG number를 공유하고 있기 때문에, CE에서 SCG 구성 요청 메시지를 수신하면 SCG number를 참조하여 다른 인트라넷의 MS에 SCG 구성을 의뢰한다.

그림 13은 본 논문에서 제안한 SCG number를 이용한 계층적 VPN의 구성의 한 예이다. 이미 초기화 과정은 이루어 졌다고 가정하고, 서로 다른 인트라넷 상에 있는 Secure Group 사이에 새로운 Secure Group을 구성하고자 하는 경우를 나타내고 있다. SFG A의 SG1과 SFG L의 SG2가 새로운 SCG를 구성하는 동작을 나타냈다. 처음에 SG1의 대표 CE인 CE1이 MS A에 SG 요청 메시지를 송신하면(①), MS A는 SG 구성 정보를 살펴보고 MS L에 요청 메시지를 송신한다(②). 요청 메시지를 수신한 MS L은 SG2의 대표 CE4에 이를 송신한다(③). CE4는 수락 메시지를 MS L에게 송신하고(④), MS L은 암호키와 암호 알고리즘을 생성하여 MS A에 송신한다(⑤). MS A는 SCG 구성을 위한 정보를 수신하면 응답 메시지를 MS L에 송신하고(⑥), 각 MS는 SCG 구성을 위하여 각 CE에 구성 정보를 송신하고(⑦) SCG topology를 수정한다.

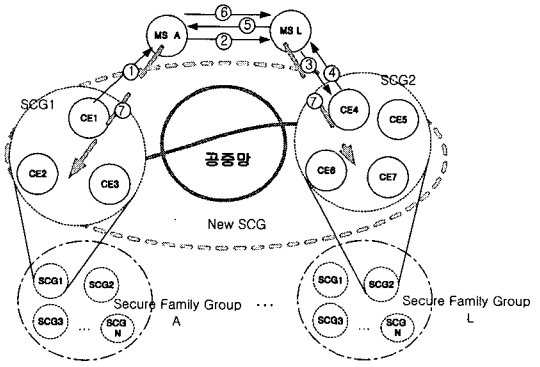

그림 13. SCG number를 이용한 계층적 vpn 구성의 예
Fig. 13. Example of hierarchical VPN configuration using SCG number.

3. 방식별 비교 분석

IV장 1.2에서 검토한 계층적 VPN 적용 방안을 비교하기 위하여, 새로운 SCG를 생성하기 위한 조건과

SFG(Secure Family Group), SG(Secure Group), SG당 CE(Communication Entity)의 수를 다음과 같이 가정한다.

- ▶ 각 CE는 모두 VPN에 참가함
- ▶ 새로운 SCG는 SG간에만 생성됨
- ▶ 모든 SG당 두개의 SG와 연결됨
- ▶ 모든 SG와 새로운 SCG를 구성함
- ▶ SFG의 수(L개), SG의 수(M개), 각 SG당 CE의 수(N개), 전체 CE의 수(LMN개)

표 3은 CE에서 관리할 최대 키의 개수를 정량적으로 나타냈다. 이 방식에서 방식 3과 방식 5는 Area-definition 방식과 Path-definition 방식을 적용함으로써 관리해야 할 키가 중복되기 때문에 키의 수가 증가하였다. 그러나 제안하는 방식은 CE의 개수에 영향을 받지 않으므로 일정한 키의 개수만 관리하면 된다. 따라서 CE에서 관리하여야 할 키의 수가 가장 적음을 알 수 있다.

그림 14는 SFG의 개수를 5개, SG의 개수를 10개로 고정한 상태에서 CE의 수를 변화시키며 CE에서 관리해야 할 최대 키의 개수를 나타냈다. 방식3과 7이 방식 1과 5와 비교하여 관리해야 할 최대 키의 개수가 적음을 알 수 있다. 특히 제안한 방식은 CE의 개수에 영향을 받지 않으므로 일정한 키의 개수만 관리하면 된다.

표 3. CE에서 관리될 최대 키의 개수
Table 3. Maximum number of key managed by CE.

	CE에서 관리할 최대 키의 개수
방식1	$(N-1)+N(M-1)+(L-1)MN+1$
방식3	$(N-1)+(M-1)+(L-1)MN+1$
방식5	$1+N(M-1)+(L-1)MN+1$
방식7	$1+(M-1)+(L-1)MN+1$
제안방식	$1+(M-1)+(L-1)M+1$

표 4는 CE에서 수행될 최대 인증 횟수를 정량적으로 표시하였으며, 그 결과를 그림 15에 나타냈다. 이 방식에서 방식 3과 방식 5는 Area-definition 구성 방식과 Path-definition 구성방식을 적용함으로써 인증 횟수가 증가하였다. 따라서 인트라넷 내부에서는 Area-definition 방식을 적용하고 인터넷 환경에는 Path-definition 방식을 적용하는 방식7을 이용하면, 인증 횟수가 적음을 알 수 있다. 제안방식에서 CE는 MS와 한번만 인증을 하면 된다. 그 이유는 처음 MS와 인증과정을 거치고, 각 인트라넷에 있는 MS 사이에 인증을 거치게 되면 각 인트라넷에 있는 MS들이 CE를 인증한 상태이므로, 새로운 SCG 구성을 위한 별도의 인증과정이 필요 없다. 따라서 CE는 자신이 속해있는 인트라넷의 MS와 한번만 인증을 하면 된다.

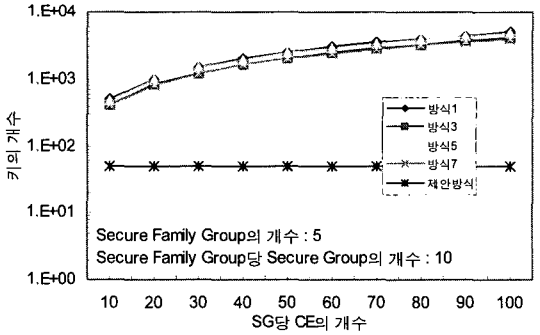

그림 14. CE에서 관리할 최대 키의 개수
Fig. 14. Maximum number of key managed by CE.

표 5. MS에서 관리할 최대 키의 개수
Table 5. Maximum key number managed by MS.

	MS에서 관리할 최대 키의 개수 $(\because A=1+\sum_{i=2}^{N-1}K),\ \binom{M}{2}={}_M C_2$
방식1	$MA+\binom{M}{2}A+\left(\binom{LM}{2}-\binom{M}{2}\right)A+MN$
방식3	$MA+\binom{M}{2}+\left(\binom{LM}{2}-\binom{M}{2}\right)A+MN$
방식5	$M+\binom{M}{2}A+\left(\binom{LM}{2}-\binom{M}{2}\right)A+MN$
방식7	$M+\binom{M}{2}+\left(\binom{LM}{2}-\binom{M}{2}\right)A+MN$
제안방식	$M+\binom{M}{2}+\left(\binom{LM}{2}-\binom{M}{2}\right)+L+MN$

표 5는 MS에서 관리할 최대 키의 개수를 정량적으로 나타냈다. 이 방식에서 방식 3과 방식 5는 Area-definition 구성 방식과 Path-definition 구성방식을 적용함으로써 관리해야 할 키의 수가 중복되기 때문에 키의 수가 증가하였다. 인트라넷 내부에서는 Area-

definition 방식을 적용하고 인터넷 환경에는 Path-definition 방식을 적용하는 방식 7을 방식 1, 3, 5와 비교하여 보면, CE의 개수가 증가함에 따라 관리할 최대 키의 개수가 가장 적음을 알 수 있다. 그러나 제안 방식은 CE의 개수에 영향을 받지 않으므로 관리할 키의 개수가 크게 증가하지 않는다. 따라서 제안하는 본 방식이 VPN 시스템 구축 시 성능면에서 효과적이다.

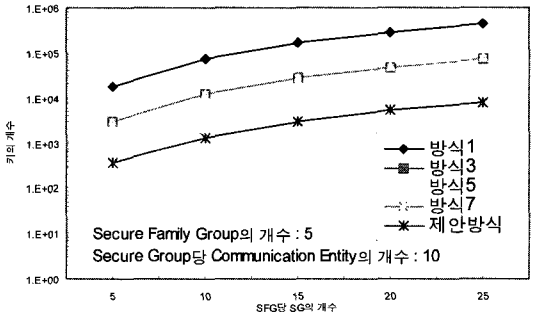

그림 16. MS에서 관리할 최대 키의 개수
Fig. 16. Maximum number of key managed by MS.

표 6. MS에서 수행될 최대 인증 횟수
Table 6. Maximum authentication number executed by MS.

	MS의 최대 인증 횟수
방식1	$MN+\binom{M}{2}N+\left(\binom{LM}{2}-\binom{M}{2}\right)N+MN$
방식3	$MN+\left(\binom{LM}{2}-\binom{M}{2}\right)N+MN$
방식5	$\binom{M}{2}N+\left(\binom{LM}{2}-\binom{M}{2}\right)N+MN$
방식7	$\left(\binom{LM}{2}-\binom{M}{2}\right)N+MN$
제안방식	$L+MN$

표 6은 VPN 구성 방식별 MS에서 수행될 최대 인증 횟수를 나타냈다. 이 방식에서 방식 3과 방식 5는 Area-definition 구성 방식과 Path-definition 구성방식을 적용함으로써 인증 횟수가 증가하였다. 제안 방식에서 MS는 인트라넷 내부의 각 CE와 인증을 하고, 다른 인트라넷에 있는 MS와 인증을 한다. 즉, SCG 구성이 요구되면 CE는 이미 MS와 인증되어 있고, 각 MS들 사이에 인증과정을 수행하였으므로 별도의 인증 없이 구성할 수 있다. 즉, 다른 인트라넷의 CE와 인증을 할 필요가 없으므로 CE의 개수에 영향을 받지 않는다. 따라서 본 제안 방식은 다른 방식보다 인증 회수가 적음을 알 수 있으며, 그림 17에 각 방식별 MS에서 인증해야 할 인증 횟수를 나타냈다.

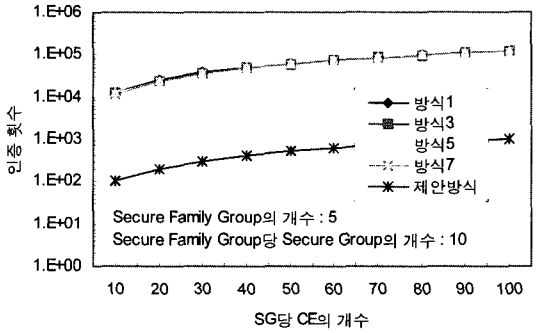

그림 17. MS의 최대 인증 횟수
Fig. 17. Maximum authentication number executed by MS.

V. 결 론

다양한 형태의 VPN을 구성하기 위하여 SCG의 개념을 적용한 계층적 VPN을 구성하고, 각 방식에 대해 가능성을 검토하였다. 인트라넷 내부에서 다양한 형태의 VPN을 구성할 때, Area-definition 방식보다 Path-definition 방식 적용이 더 효율적이다. 그러나 인터넷을 통해 인트라넷 VPN 구성에는 Area-definition 방식보다 Path-definition 방식을 사용하여야 한다.

본 논문에서는 SCG number를 이용하여 논리적으로 인터넷에 Area-definition을 적용한 계층적 VPN 구성 방법을 제시하고, 그의 특성을 분명히 하였다.

계층적 VPN 구성 방법으로 인트라넷 VPN 환경에서 각 SCG를 정의하고, 5가지 방법(표 3에 제시)에 대해 검토하였다. 검토 결과 기존 방식(표 3의 방식 1, 방식 3, 방식5, 방식 7)에서는 인트라넷 내부(Secure Family Group)에서는 Area-definition 방식을 적용하는 것이 우수하다. Path-definition 방식과 Area-definition 방식을 혼합하여 사용하는 경우, SG(Secure Group) 간에 Area-definition 방식을 적용하면 CE와 MS에서 관리할 최대 키의 개수와 최대 인증 횟수가 상대적으로 적음을 알 수 있다. 그리고 Secure Family Group에는 Area-definition을 적용할 수 없으므로 Path-definition

방식만을 적용하여야 한다.

그러므로 본 논문에서는 SCG number를 이용하여 계층적으로 VPN를 구성 할 경우 기존 방식에 비하여 관리할 키의 개수와 인증 횟수가 적음을 정량적으로 분석하고, 본 방식이 VPN 구성에서 기존의 다른 방식보다 성능 개선 가능성을 나타냈다.

따라서 제안한 계층적 VPN이 기존 방식으로 구성한 VPN과 비교하여 인증에 의한 키의 수와 인증 횟수를 관점에서 볼 때 지연과 트래픽 처리 특성면에서 개선된 방식임을 알 수 있다. 금후 본 개념을 적용하여 실제 구현하는 연구가 필요하다.

참 고 문 헌

[1] 한국정보보호센터, "IP 계층과 응용계층에서의 VPN 보안기술 표준(안)", March 1999.

[2] B. Gleeson, A. Lin, J. Heinanen, G. Armitage, A. Malis, "A Framework for IP Based Virtual Private Networks", RFC 2764, February 2000.

[3] P. Rapalus, "Issues and Trends: 1998 CSI/FBI Computer Crime and Security Survey", CSI Press Release, March 1998.

[4] A. Watanabe, S. Seno, Y. Koui, T. Ideguchi, M. Yabe, "Realization Method of secure Communication Groups using Encryption", Transactions of Information Processing Society of Japan V.38 N.4, April 1997.

[5] A. Watanabe, T. Inada, T. Ideguchi, I. Sasase, "Proposal of Group Search Protocol Making Secure Communication Groups for Intranet", ICC 2000, June 2000.

[6] S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[7] A. Watanabe, et al., "Proposal of Group Search Protocol making the Realization of Closed Communication Groups easy", CSS99, Oct. 1999.

[8] David McDysan, "VPN Application Guide", John Wiley & Sons Inc., 2000.

[9] P.Ferguson, G.Huston, "What is VPN?", The Internet Protocol Journal, April, 1998

저 자 소 개

朴 贊 祐(正會員)

1995년 3월~1999년 2월 한국외국어대학교 전자공학과 학사, 1999년 3월~2001년 2월 한국외국어대학교 대학원 전자정보공학과 석사, 2001년 3월~현재 한창시스템 기술연구소 소프트웨어팀 연구원, 주 관심분야는 네트워크 보안, 인터넷, VPN 등

韓 致文(正會員)

1970년~1977년 경북대학교 전자공학과 학사, 1981년~1983년 연세대학교 전자공학과 석사, 1987년4월~1990년 9월 일본 동경대학 대학원 전자정보공학과 공학박사, 1977년 2월~1983년3월 한국과학기술연구원(KIST) 연구원, 1983년 4월~977년 2월 한국전자통신연구원(ETRI) 책임연구원 교환기술연구단 계통연구부장 역임, 1977년 3월~현재한국외국어대학교 전자정보공학부 교수, 주 관심분야는 초고속 교환 방식 및 통신망 구조, 광인터넷, 네트워크 보안 등