A Proposal for a Remote Access Method using GSCIP and IPsec

Keisuke Imamura, Hidekazu Suzuki, Akira Watanabe
Graduate School of Science and Technology, Meijo University
1-501 Shiogamaguchi, Tempaku-ku, Nagoya, 468-8502 JAPAN

***Abstract*— Demand for the system to make secure remote access from the Internet to enterprise networks has been increasing. However, the security of the existing remote access methods is vulnerable in Internets, although it is robust on the Internet. In order to solve this problem, we have studied a remote access method that uses IPsec and GSCIP in combination. This method can realize End-to-End secure communication not only for the Internet but also for Intranets.**

I. Introduction

Access to enterprise networks from the Internet is becoming common. However, there exist many threats, such as eavesdropping, modification and masquerade on the Internet. In order to protect the communication from these threats, systems based on remote access VPNs (Virtual Private Networks) are widly utilized. Typical remote access methods are Point-to-Point Tunneling Protocol (PPTP) [1], Layer 2 Tunneling Protocol (L2TP) [2], IPsec [3] and Secure Socket Layer (SSL) [4].

Since the security level of PPTP and L2TP is rather low, IPsec and SSL are usually used for enterprise networks. However, because IPsec has many setting items, the management load gets heavy when the number of users increases. In case of SSL, its application is limited because it is defined between a transport layer and a session layer. Although the security level of both methods is high on the Internet, security in intranets is not taken into account. Nevertheless, threats also exist in intranets. It is thus desirable to encrypt communications from End-to-End even in the case of remote accesses. Although an IPsec transport mode may be used for realizing End-to-End cipher communication, UDP encapsulation is required to traverse a Network Address Translator (NAT) [5], and then, the security level gets lower.

In intranets, a very simple authentication method using a user name and a password is widely used. One may think that IPsec is useful for intranets, but it is in reality not suitable because the management load is very high in case system configurations frequently change. We have been proposing a new network architecture called “GSCIP” (Grouping for Secure Communication for IP) [6], which has both security and flexibility. In GSCIP, communication groups are defined by way of common keys, and the groups are independent of IP addresses. Authentication and cipher communication are realized with the common keys. In this paper, a remote access method that enables End-to-End cipher communication is proposed, based on the combination of GSCIP and IPsec.

In Section II, existing technologies are described. We present the remote access method using GSCIP and IPsec in Section III, and describe its evaluation in Section IV. Finally, we summarize the paper in Section V.

II. Existing Technologies and Their Problems

A. IPsec-VPN

IPsec is a security protocol which can be used for any purposes on the TCP/IP. It is implemented in the network layer and standardized in Internet Engineering Task Force (IETF).

Internet Key Exchange (IKE) [7] is a protocol which generates Security Association (SA) of IPsec automatically. IKE exchanges information about algorithm types and the seeds of a key on the Internet. Fig. 1 shows a remote access system using IPsec. An IPsec-VPN device is installed at the entrance of the enterprise network. A remote terminal executes IKE with the VPN device, and creates SA. After that, IPsec packets are encrypted according to the security policy.

In the IPsec-VPN, End-to-End secure communication is not realized. Since an IPsec tunnel is created between a remote terminal and the VPN device, communications in the intranet is in clear text. Although the IPsec transport mode can be used for End-to-End cipher communication, it is necessary to encapsulate IPsec packets with UDP in order to traverse a NAT [8]. In this method, UDP parts are not within the scope of integrity, and it can not ensure the original security level of IPsec.

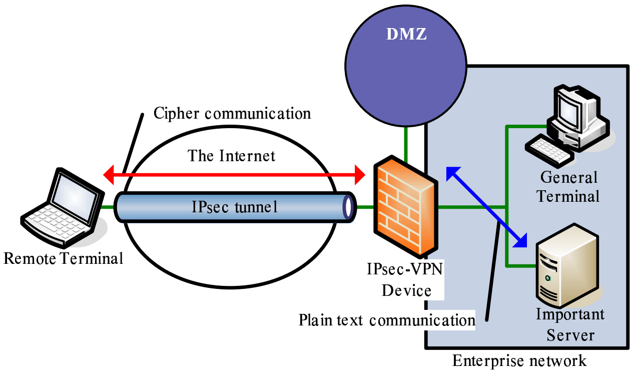


Fig. 1. Remote access system using IPsec.

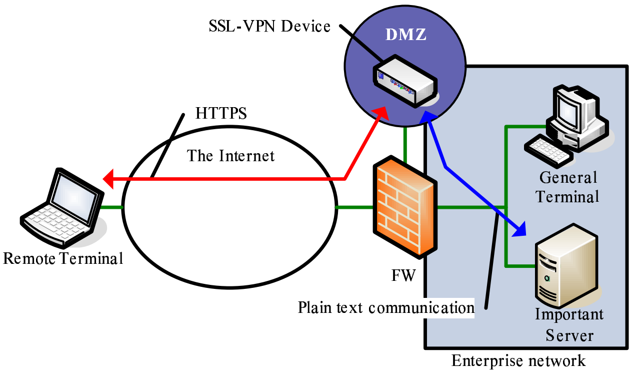


Fig. 2. Remote access system using SSL.

B. SSL-VPN

SSL is a protocol defined at the boundary of a session layer and a transport layer, and this can be used for applications like HTTP and FTP. SSL-VPN is a VPN technology that uses SSL for the purpose of encryption. Most of web browsers support SSL as the standard, and it is easy to use.

A remote access system using SSL is shown in Fig. 2. A SSL-VPN server is set on the demilitarized zone (DMZ) and a remote terminal accesses the SSL-VPN server using a web browser. The path between the remote terminal and the SSL-VPN server is secure because HTTPS is used. In the wake of the user authentication, link lists of resources are displayed on the remote terminal. When a user chooses a link, the SSL-VPN server accesses the corresponding server using each application protocol. The SSL-VPN server converts the protocol between the applications and HTTPS. In this method, the remote terminal needs only a web browser. However, the application is limited because protocol conversion functions are required in the SSL-VPN server. Such applications that use UDP, dynamic TCP port numbers, or plural TCP sessions can not be used. For work from home, there exists a strong demand for the use of applications adopted on the job, but SSL-VPN may not be used to meet such demand.

III. Proposed Method

A. Purpose of the proposed method

Although the existing remote access methods are secure on the Internet, the security in the intranet is almost ignored. At present, a very simple user authentication based on the user name and a password is used in the intranet. Nevertheless, network threats also exist in intranets, and internal crimes are constantly being reported these days. IPsec might be one of the solutions for solving the problem.

IPsec transport mode is used to from individual-base communication groups. Although this method makes it possible to define very fine groups, the management load will increase in proportion as the scale of the system gets larger. IPsec tunnel mode is used to from unit-based communication groups. What is needed in this method is more installation of security functions to routers, but it is difficult to define very fine communication groups. In intranets, there often exist both Individual-based and Unit-based communication groups together. In IPsec, transport mode and tunnel mode are not compatible, and it is not suitable for intranets because the management load gets heavier when both types of communication groups coexist.

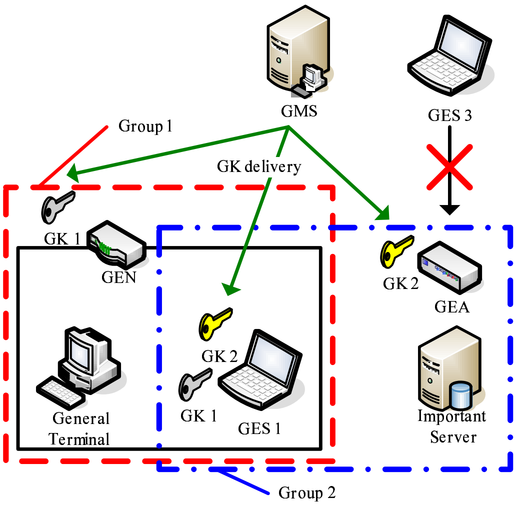


Fig. 3. Principle of communication groups with GSCIP.

To solve the problem, we have been proposing a new communication architecture called “GSCIP” (This is pronounced like “G-skip”) in intranets that has both flexibility and security. In this paper, we combine the technologies of GSCIP and IPsec, and realize remote access that can achieve End-to-End cipher communication.

B. Principle of GSCIP

GSCIP is a network architecture which has both flexibility and security. The principle of the communication groups with GSCIP is shown in Fig. 3.

The construction element for the communication groups in GSCIP is called “GE” (GSCIP Element). There are three types of GEs; namely, a host-type GES (GE realized by Software) which is installed in a terminal, a router-type GEN (GE for Network) which acts as a router, and a bridge-type GEA (GE realized by Adapter) which is set in front of the server and acts as a GES. GEN protests all general terminals (Term) of its sub-network. GSCIP defines a set of GEs which possess the same common encryption keys of the same communication group. This encryption key is called a “group key” (GK). With this method, communication groups can be logically defined without depending on IP addresses. Communication among members of the same group is encrypted with the GK. In Fig. 3, GEA belongs to the group 2 and it is possible to refuse the access from GES3 which is not in the same group. An administrator defines communication groups at the Group Management Server (GMS), and the GMS distribute group information corresponding to the group keys. Communications between the GMS and GEs is authenticated and encrypted with

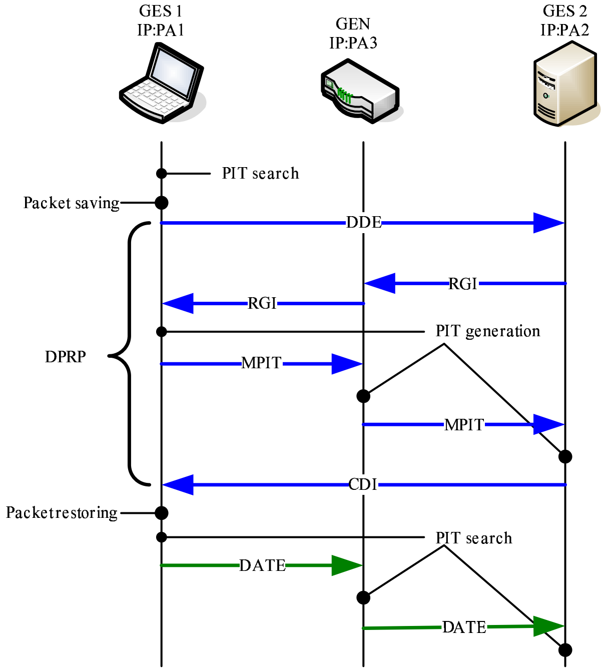


Fig. 4. DPRP sequence.

the public keys with certainty. GKs are updated periodically.

C. Outline of DPRP

Dynamic Process Resolution Protocol (DPRP) [9] is one of the protocols which organize GSCIP. GEs learn network configurations and define their operations automatically. Each GE handles packets according to its own Process Information Table (PIT). In PIT, process information (encrypt/decrypt, relay, discard) is described. Connection ID (CID) is used for searching PIT. DPRP is executed in advance of communication between terminals. DPRP sequence is shown in Fig. 4.

When a GE sends a packet, it searches its PIT, and handles the packet according to the PIT. If no corresponding PIT is found, it saves the sending packet temporarily, and starts DPRP sequence. Four kinds of packets, namely DDE (Detect Destination End GE), RGI (Report GE Information), MPIT (Make Process Information Table), and CDN (Complete DPRP Negotiation), which are all based on ICMP, are used for DPRP. CID of the sending packet is set in DDE, and is sent to the destination terminal. GES2 which receives DDE becomes a destination End-GE and it returns RGI. The user ID and group information are set in RGI. When GEN which is on the way of the communication path relays RGI, it adds its own group information to the packet. GES1 which receives RGI becomes a source End-GE, and it determines individual process information of GEs from the collected information. GES1 sets the determined process information in MPIT, and sends it to GES2. GEN and GES2 which receive MPIT pick up the process information of its own, and generate PITs. GES2 sends back CDN to GES1 in order to notify the completion of DPRP. GES1 which receives CDN restores the temporarily saved packet, and communication starts.

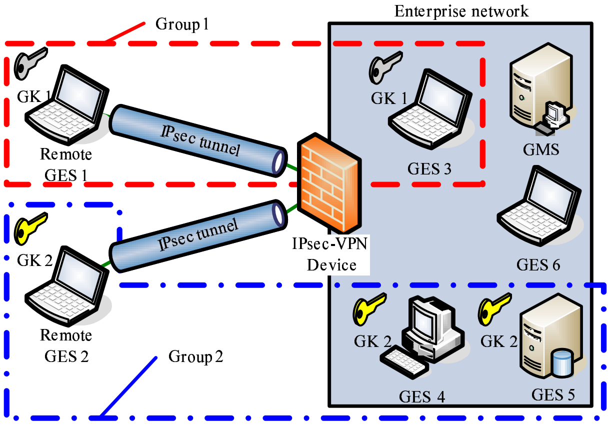


Fig. 5. Configuration of the proposed method.

The packet thereafter are handled according to the process information in PIT which indicates “encrypt/decrypt”, “relay”, or “discard”. We assume that Practical Cipher Communication Protocol (PCCOM) [10] is used as a cipher communication technology.

D. Remote access by the proposed method

The configuration of the proposed method is shown in Fig. 5. GSCIP and IPsec are used together. First, a remote GES executes IKE with an IPsec-VPN device, and creates an IPsec tunnel. Then, the remote GES requests for a GK to the GMS. The remote GES is authenticated by the GMS with the public keys. Corresponding group information and the GK are delivered from the GMS to the remote GES. After that, the remote GES executes DPRP with the GES in the intranet and the communication starts.

With the IPsec tunnel, remote GESs are incorporated into the enterprise network, and the secure End-to-End communication is realized with PCCOM in GSCIP. The IPsec tunnel part is double encrypted with IPsec Encapsulating Security Payload (ESP) [11], [12] and PCCOM.

IV. Evaluation

Comparison of the existing technologies with our proposed method is shown in Table I. The “IPsec tunnel mode” is a method to create a tunnel (IPsec tunnel) between a remote terminal and the VPN device. In this method, communications in the intranet side is in clear text, and thus, the security is vulnerable. The “IPsec transport mode” is a method to implement IPsec also at the terminal of the enterprise LAN, and perform End-to-End cipher communication. However, this method entails encapsulation of IPsec packets with UDP in order to traverse a NAT, and accordingly, the security level of IPsec gets lower. Also, the management load becomes large if the system gets large. The SSL-VPN is a method where the SSL-VPN device installed on the DMZ makes access to the server of the enterprise as a proxy. The path between the remote terminal and the SSL-VPN server is secure because

TABLE I

COMPARISON OF EXISTING TECHNOLOGIES WITH OUR PROPOSAL SYSTEM

	IPsec tunnel mode	IPsec transport mode	SSL-VPN	Proposed method
Method	A remote terminal and the VPN device are connected by IPsec tunnel.	A remote terminal and the server in the intranet are connected by IPsec transport mode.	The VPN device and the SSL-VPN device are connected by SSL.	A remote terminal and the VPN device is connected by IPsec tunnel mode, and the remote terminal and the server are connected by GSCIP.
Security	× Communications in the intranet is in clear text.	△ IPsec security level degrades due to UDP encapsulation.	× Communication in the intranet is in clear text.	○
Management loads	○	× Management load increase, when the system becomes large.	× Management load increase, when the system becomes large.	△ Management loads of GSCIP are small.
Applications	○	○	× Applications are limited.	○

HTTPS is used. However, because the communication on the intranet side is in clear text, its application is limited. Our "Proposed method" applies both IPsec and GSCIP and realizes End-to-End cipher communication. Since GSCIP generates process information dynamically, the management loads does not increase so much. Also, application is not limited.

V. CONCLUSION

Although the existing remote access methods are secure on the Internet, the security in the intranet is almost ignored. In the intranet, a user name and a password are usually used for user authentication, but this method is vulnerable. To solve this problem, we have been proposing GSCIP that have both flexibility and security. In this paper, we have proposed a remote access method that uses IPsec tunnel mode and GSCIP together. The increase of the management load is small and the application is not limited. In future, we will perform a trial run and evaluate the system.

REFERENCES

[1] K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little, and G. Zorn, "Point-to-point tunneling protocol (pptp)," RFC 2637, July 1999.

[2] W. Townsley, A. Valencia, A. Rubens, G. Pall, G. Zorn, and B. Palter, "Layer two tunneling protocol "l2tp"," RFC 2661, Aug. 1999.

[3] S. Kent and K. Seo, "Security architecture for the internet protocol," RFC 4301, Dec. 2005.

[4] T. Dierks and C. Allen, "The tls protocol version 1.0," RFC 2246, Jan. 1999.

[5] P. Srisuresh and K. Egevang, "Traditional ip network address translator (traditional nat)," RFC 3022, Jan. 2001.

[6] H. Suzuki, M. Takeuchi, N. Kato, S. Masuda, and A. Watanabe, "A proposal of secure communication architecture gscip realizing flexible private network," in *Proc. Symposium on Multimedia, Distributed, Cooperative and Mobile Systems 2005 (DICOMO2005)*, vol. 2005, no. 6, July 2005, pp. 441–444.

[7] P. Hoffman, "Algorithms for internet key exchange version 1 (ikev1)," RFC 4109, May 2005.

[8] A. Huttunen, B. Swander, V. Volpe, L. DiBurro, and M. Stenberg, "Udp encapsulation of ipsec esp packets," RFC 3948, Jan. 2005.

[9] H. Suzuki and A. Watanabe, "Implementation and its evaluation of dynamic process resolution protocol in flexible private network," *IPSJ Journal*, vol. 47, no. 11, pp. 2976–2991, Nov. 2006.

[10] S. Masuda, H. Suzuki, N. Okazaki, and A. Watanabe, "Proposal for a practical cipher communication protocol that can coexist with nat and firewalls," *IPSJ Journal*, vol. 47, no. 7, pp. 2258–2266, July 2006.

[11] S. Kent, "Ip encapsulating security payload (esp)," RFC 4303, Dec. 2005.

[12] V. Manral, "Cryptographic algorithm implementation requirements for encapsulating security payload (esp) and authentication header (ah)," RFC 4835, Apr. 2007.

IEEE TENCON 2007

Oct.30 – Nov.2, 2007

Taipei International Convention Center, Taipei, Taiwan

A Proposal for a Remote Access Method using GSCIP and IPsec

Keisuke Imamura, Hidekazu Suzuki and Akira Watanabe

Graduate School of Science and Technology,

Meijo University, JPAPN

Background

- Increase of
  - Wireless Access Networks
  - Home Workers

➡ It is becoming popular to access an enterprise network from the Internet

Eavesdropping, Falsification and Spoofing

- Remote access VPN (Virtual Private Networks) is used widely

⬇

Secure communication on the Internet

Background

- Security threats also exist in an enterprise network
  - Very simple authentication using a user name and a password
  - Most communications are performed in clear texts

Network crimes by insiders are often reported

Eavesdropping, Falsification
Spoofing

A proposal : End-to-End secure communication
that covers the Internet and the Intranet

Overview of IPsec-VPN

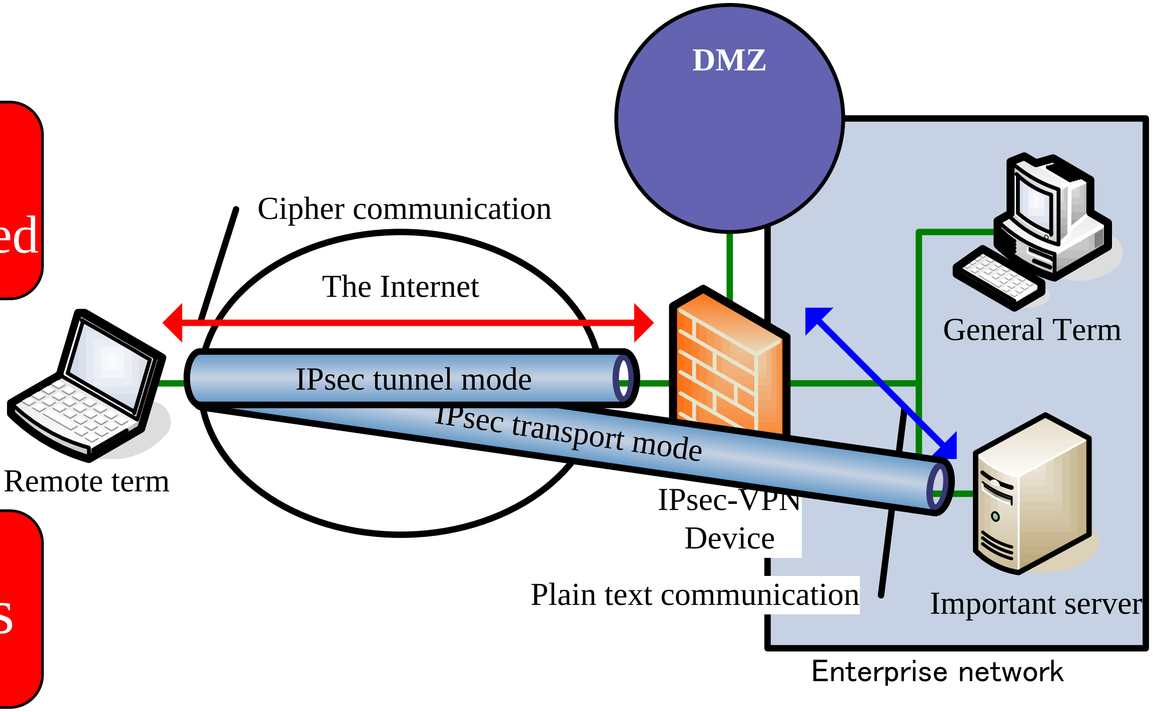
- IPsec Tunnel Mode
  - End-to-GW secure communications
- IPsec Transport Mode
  - End-to-End secure communications

Tunnel mode

End-to-End secure communication is not realized

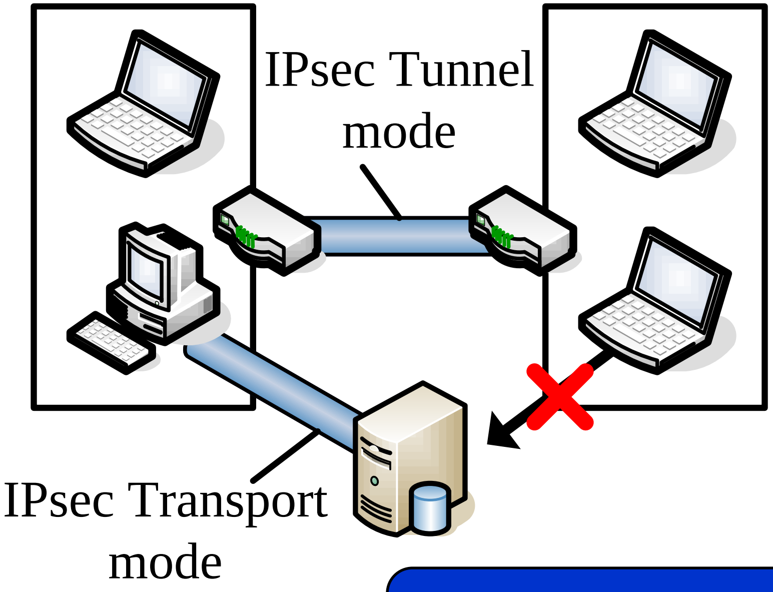
Transport mode

Security level degrades



Security measures in the intranet

- Most communications are clear texts in intranets
  - Transport mode and Tunnel mode are NOT compatible
  - Management loads become quite large

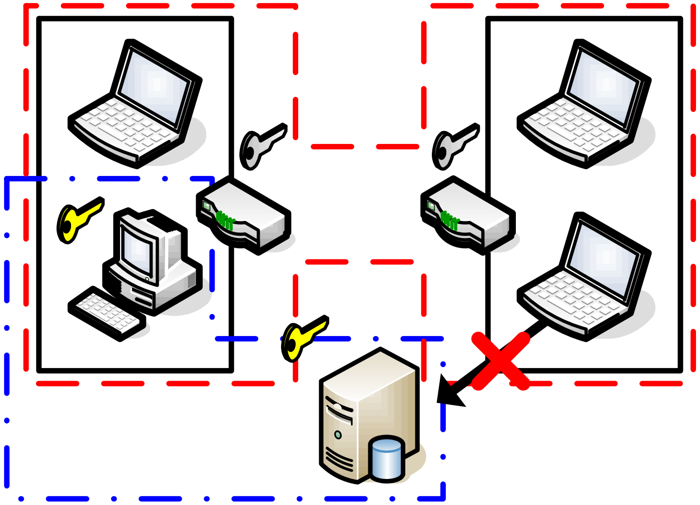


IPsec is hardly spread in intranets

GSCIP（Grouping for Secure Communication for IP）

Outline of GSCIP

- GSCIP is a network architecture which has both security and flexibility
- Terminals are belonged to several groups
  - The communication between the same groups is encrypted by a common key
  - Requests from different groups can be rejected



DPRP : Dynamic Process Resolution Protocol

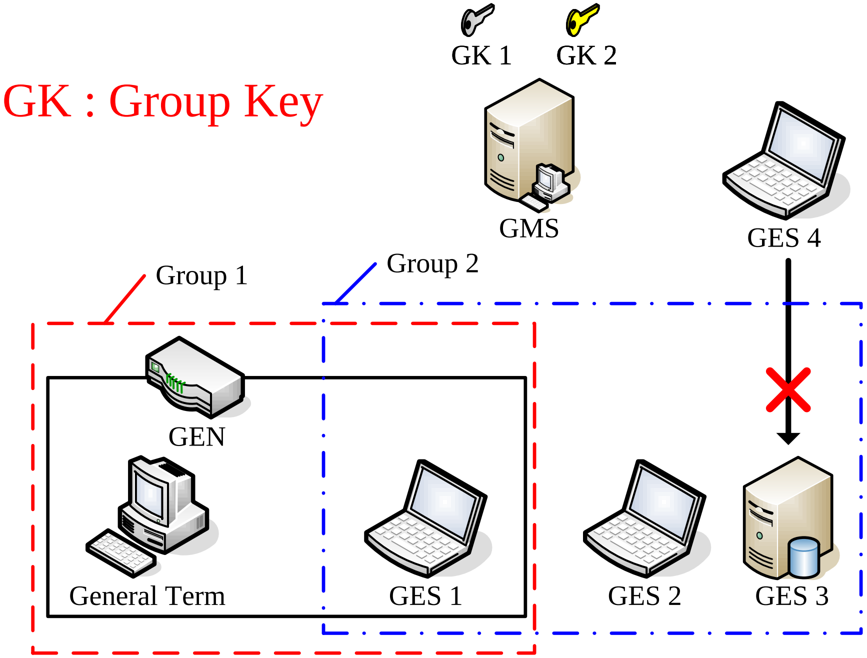
DPRP is our original protocol
is performed between terminals

□ Authentication between terminals
□ Process information in each terminal
is created by DPRP

Behavior of GSCIP

- Components of GSCIP
  - GE (GSCIP Element)
    - GES : (GE realized by Software) : Host-type GE
    - GEN : (GE for Network) : Router-type GE
  - GMS (Group Management Server)

GK : Group Key

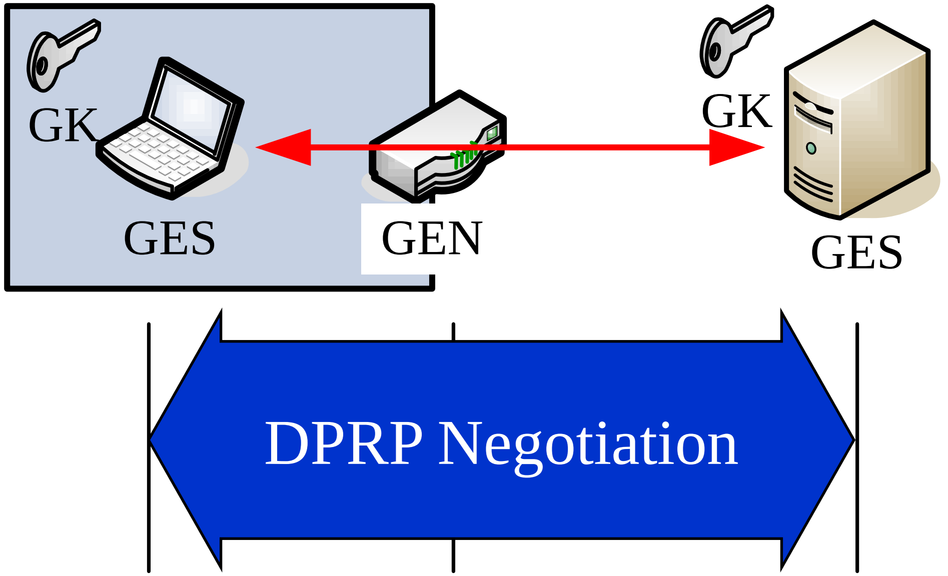


- GMS
  - □ Authenticates each GE
  - □ GK delivery (Encryptions with public keys)

■Communication groups are maintained even if terminals change their locations
■The definition of groups are independent from IP addresses

Outline of DPRP

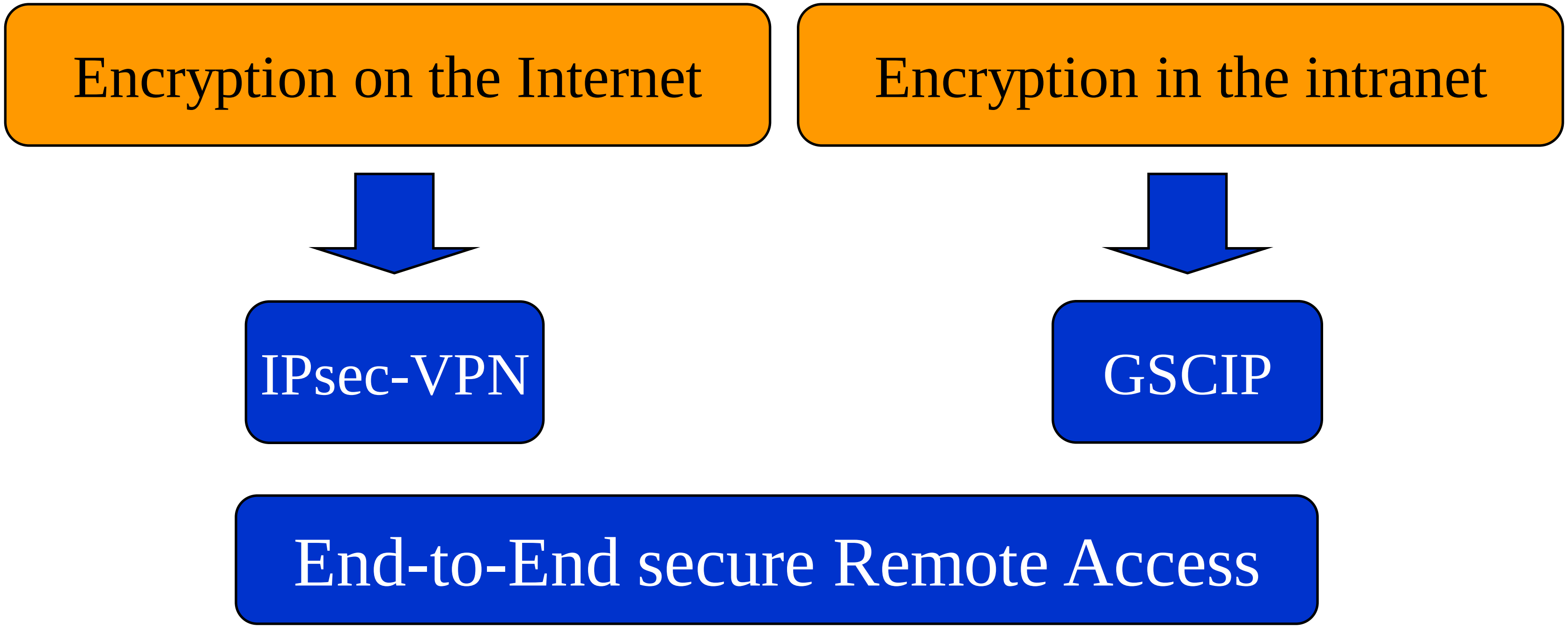
- DPRP is one of the protocols which organize GSCIP
  - Authentication between terminals
  - Exchange in group numbers, key information and Operation Mode
  - Decides Process information



Communication is performed between GEs based on the Process Information

Purpose of the proposal method

- End-to-End cipher communications
- Suppression of the increase of management loads



Encryption on the Internet

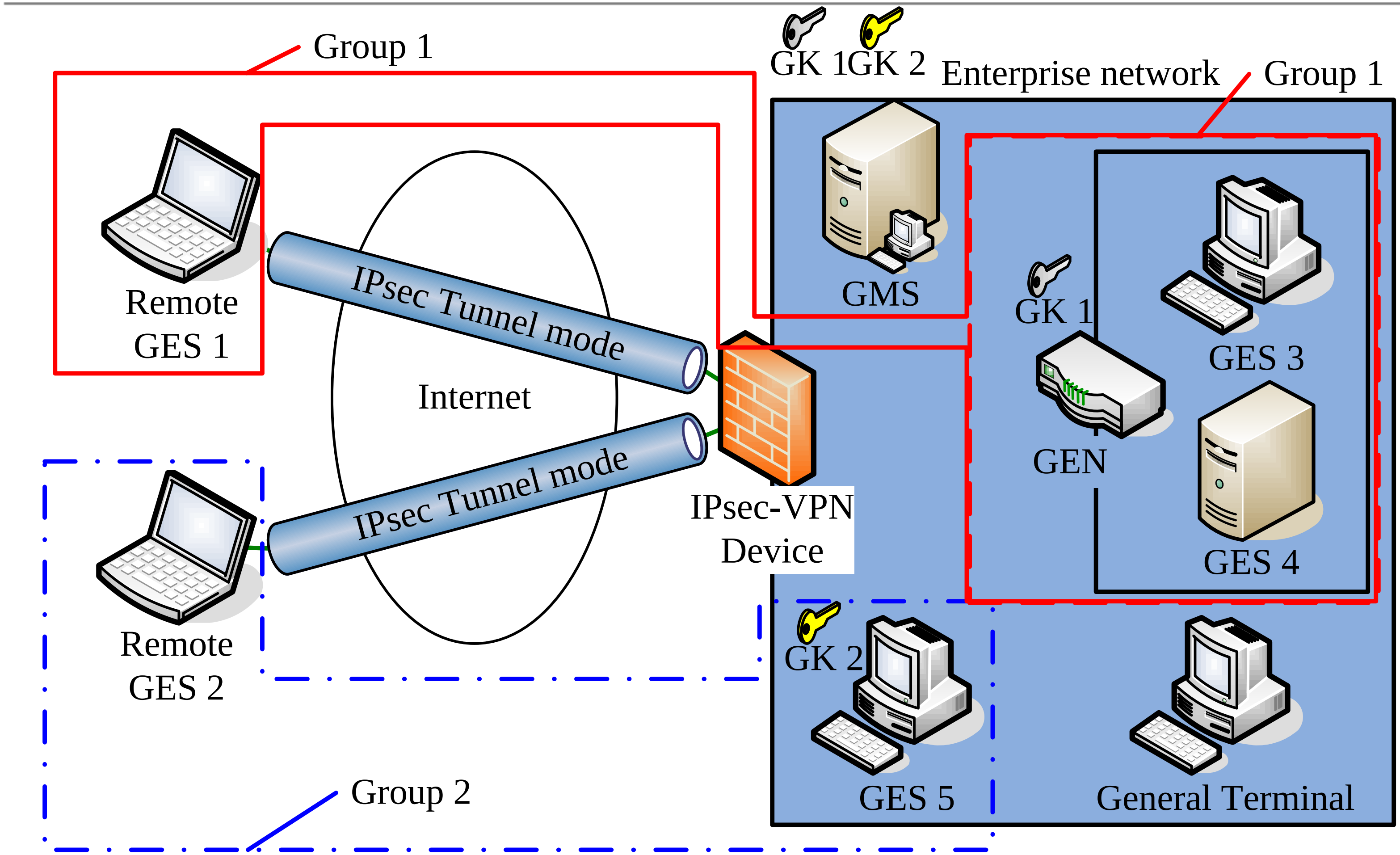
Encryption in the intranet

IPsec-VPN

GSCIP

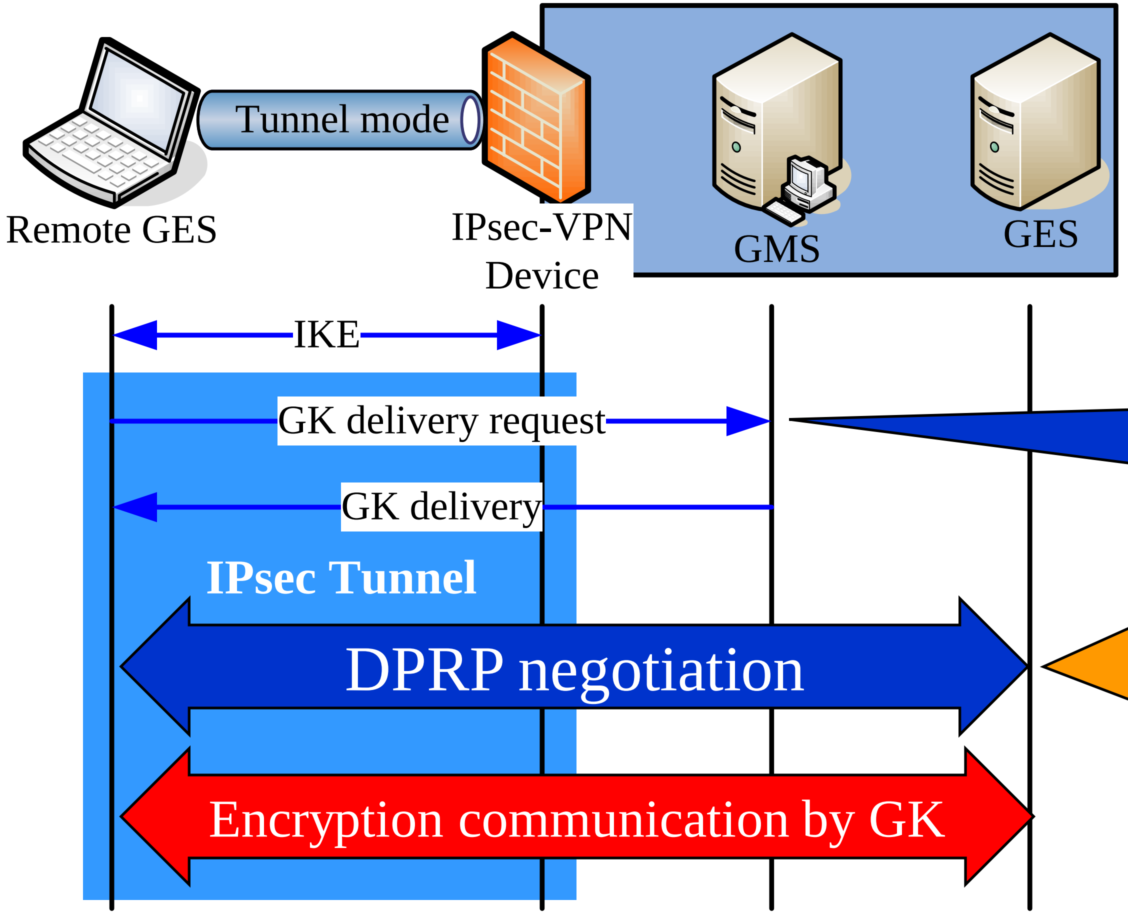
End-to-End secure Remote Access

Configuration of the proposed method



Remote terminals are incorporated into GSCIP

Sequence of the proposed method



◆Authentication of GES
◆GK delivery

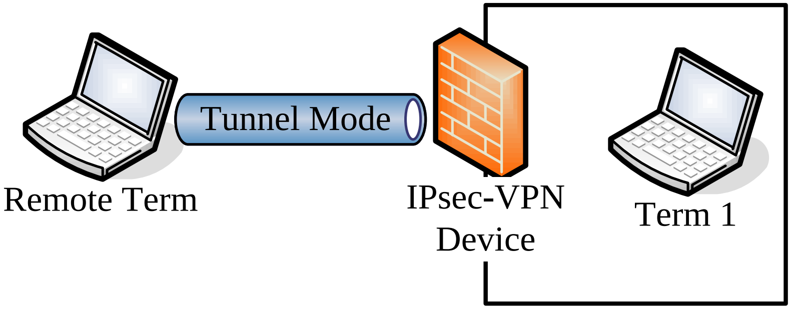
End terminals execute DPRP, and authenticate each other with the GK

End-to-End secure Remote Access is realized

Evaluation ~Setting items~

IPsec Tunnel mode

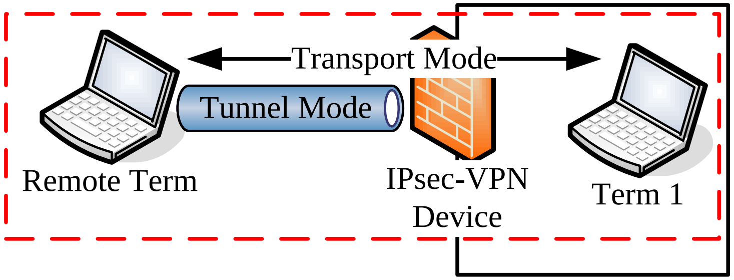
	Pre-Shared Key	Security Policy	IKE
Setting items	Identifier Pre-Shared Key	Identifier Policy （IPsec/Discard/None） Protocol（ESP/AH） Mode（Transport/Tunnel） Policy level etc.	Identifier Exchange Mode Encryption Algorithm Hash Algorithm Authentication Method DH Group etc.
The number of items	2	16	12

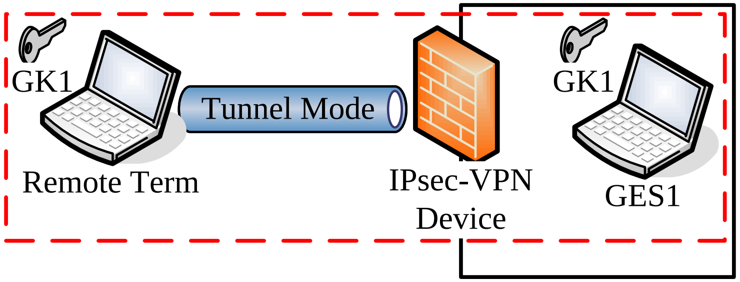


The total of 30 setting items are needed in a Tunnel mode

Evaluation ~Setting items~

	Combination of Tunnel mode and Transport mode	Combination of Tunnel mode and GSCIP
Setting items	■Setting of Tunnel mode : 30 items □Pre-Shared Key : 2 items □Security Policy : 14 items □IKE : 12 items	■Setting of Tunnel mode : 30 items □GSCIP : 5 items
The number of items	30 ＋ 28 items	30 ＋ 5 items





Setting items increase according to the number of remote terminals

Evaluation

	Tunnel mode	Combination of Tunnel mode and Transport mode	Proposed method
Strength of security	× Clear texts in intranets	○ End-to-End secure communications by IPsec	○ End-to-End secure communications by GK
Management loads	○	×	△
	30 items	30 items ＋ N×28 items	30 items ＋ N×5 items

N : The number of remote terminals

Conclusion

- The secure remote access method has simple management is proposed
  - It can be realized with the combination of GSCIP and IPsec
    - End-to-End secure communication
    - Few management loads

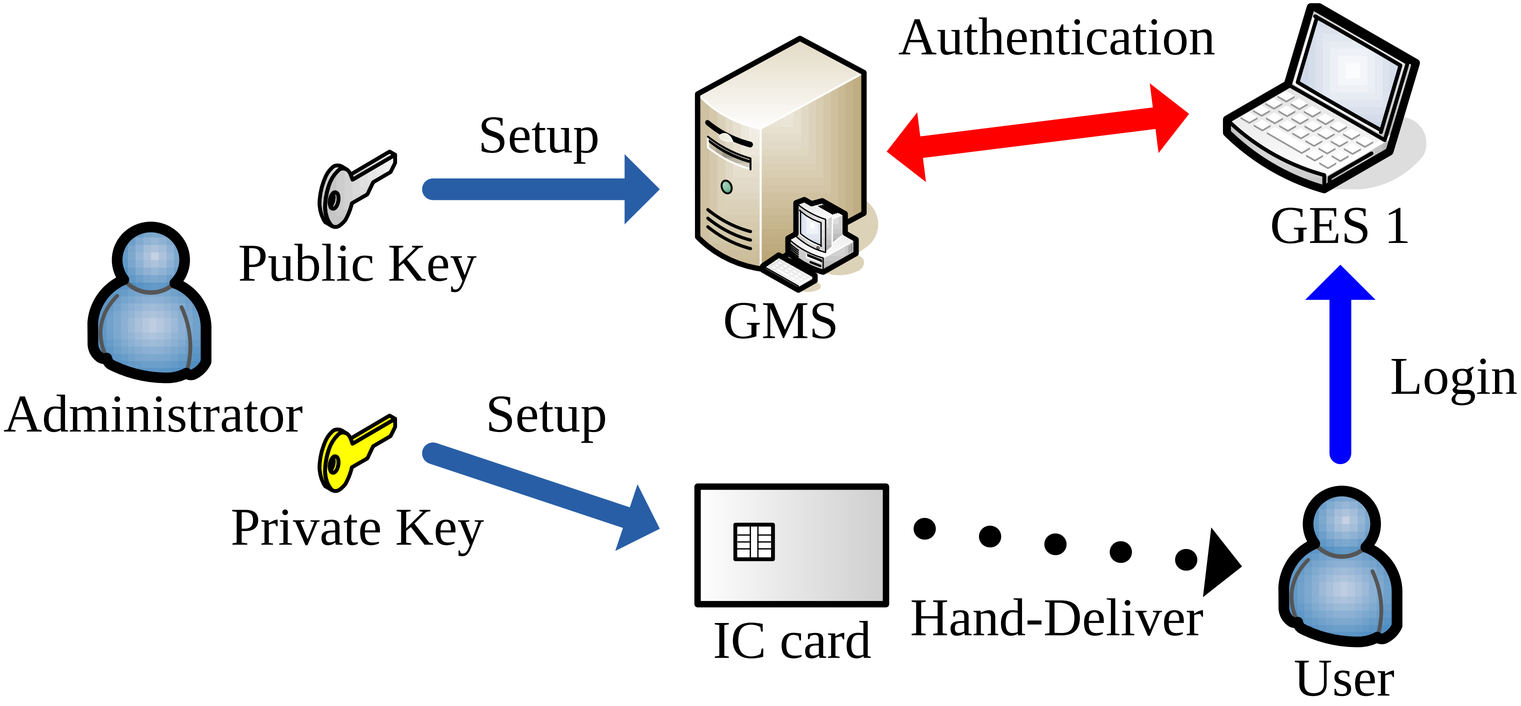
- Future work
  - Implementation
  - Performance evaluation

Appendix

When is a Public key delivered to the users?

[A] At the time of the system introduction and the user addition

- The login system with IC card
  - The administrator setup a Private/Public key in the IC card/GMS



Overheads of DPRP and IKE

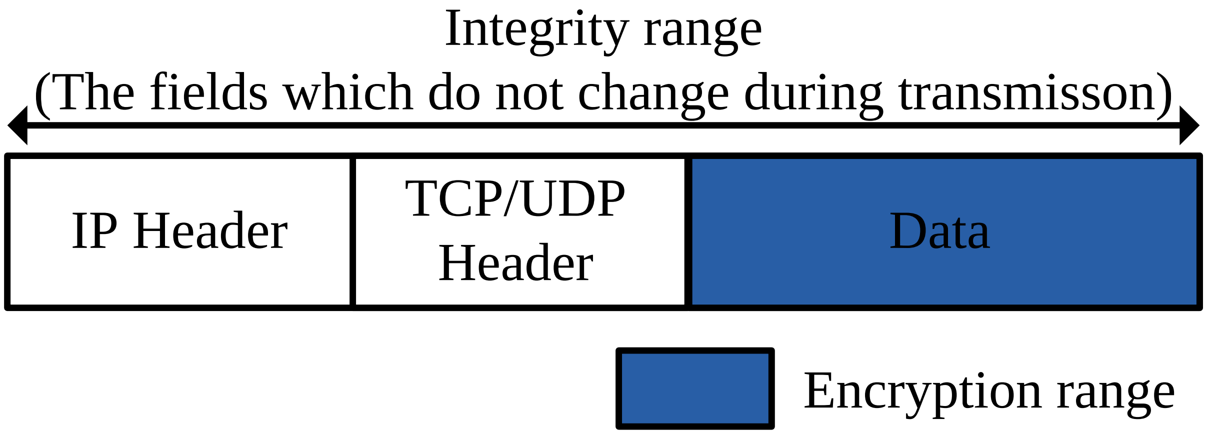
	DPRP	IKE
The negotiation	1,012 ms	1,105,954 ms
The start up time	1,040 ms	2,994,033 ms

- The negotiation time
  - DPRP : GE gets GKs from GMS in advance
  - IKE : Secret key is generated with Diffie-Hellman Key Exchange
    - Include the public key operation
- The start up time
  - DPRP : The 1st TCP packet is kept in the kernel
  - IKE : The 1st packet is discarded

TCP retransmission process works

How much is the degradation of a throughput?

- Encrypts only the portion of user date, in GSCIP



Integrity range
(The fields which do not change during transmisson)

IP Header	TCP/UDP Header	Data

🟦 Encryption range

FTP download time

500MB of file is downloaded

Normal	GSCIP	IPsec ESP
13.94 sec	20.22 sec	43.43 sec

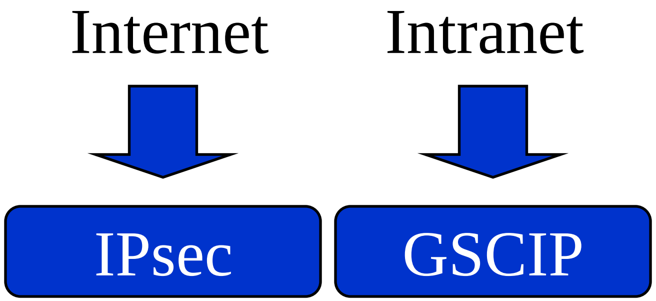
There are few degradations of a throughput as compared with IPsec

Why does it use that combination of GSCIP and IPsec?

- IPsec is strong security
  - IPsec is used for encryption on the Internet
    - Need so many setting items
- There needs a very few setting items in GSCIP
  - It can coexist with existing systems such as NAT, firewalls

	IPsec	GSCIP
Secrecy	◎	○
Identity confirmation	◎	○
Integrity assurance	◎	○
NAT	△	○
Firewalls	△	○
Fragment	△	○
Traffic analysis	○	△

Packets can be filtered as usual



The difference in the setting items of GSCIP and IPsec

IPsec/IKE	Pre-Shared Key	Security Policy	IKE
Setting items	Identifier Pre-Shared Key	Identifier Policy （IPsec/Discard/None） Protocol （ESP/AH） Mode（Transport/Tunnel） Policy level etc.	Identifier Exchange Mode Encryption Algorithm Hash Algorithm Authentication Method DH Group etc.
The number of items	2	16	12

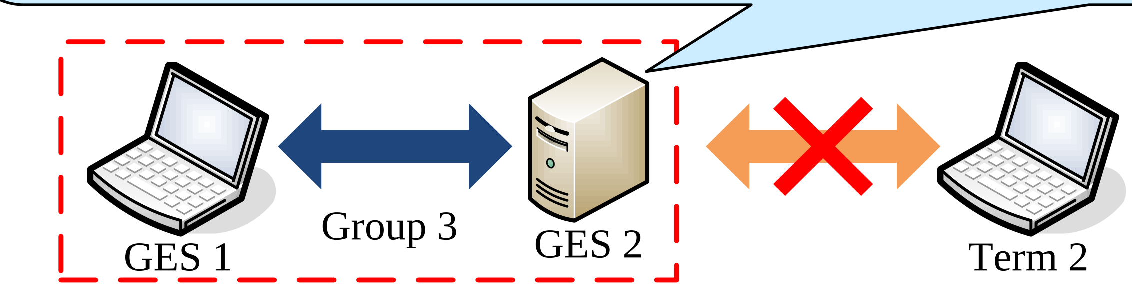
GSCIP/DPRP	Group Key		GE Information
Setting items	Group Number Key version Group Key		Operation mode (OP/CL) Group Number
The number of items	3		2

GSCIP ~Communication mechanism~

- Based on Process Information Table (PIT)

Information in PIT of GES 2

IPDST	PROC	Group Number	Ver.
GES 1	Encrypt	3	102
Term 2	Discard	---	---



- If process information exits : Handle the TCP/UDP packet
- No process information exits : Generate PIT with DPRP negotiation