Virtual Private Network – VPN

IPSec Testing:

Functionality、Interoperability and Performance

Johnnie Chen

Project Manager of Network Security Group

Network Benchmarking Lab

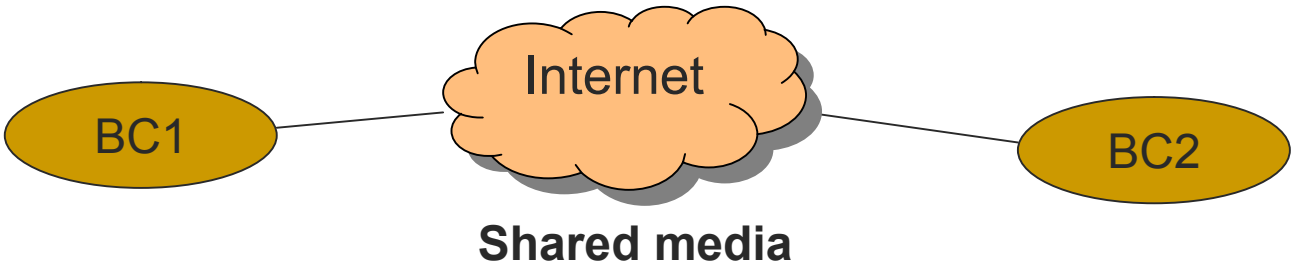
Outline

- What is VPN ? Why we need VPN ?
- IPSec Background
- Why IPSec VPN ? =>Functionalitliy
- What’re the critical issues in IPSec VPN
  =>Interoperability and Performance
- IPSec Functionality Testing
- IPSec Interoperability Testing
- IPSec Performance Testing

What is VPN ? Why we need VPN ?

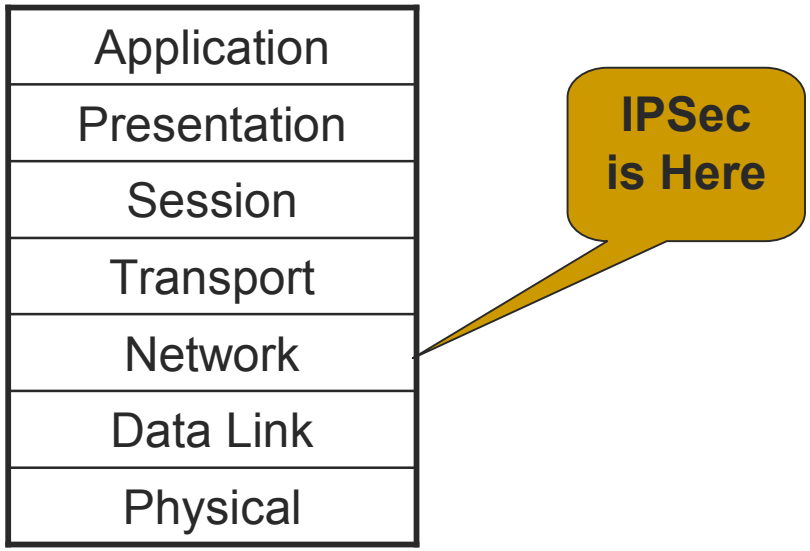
- Network: a way to communicate with others
- Private Network: a way to communicate with others in private (privacy and authenticity)

- Virtual Private Network: a way to set up private networks over shared infrastructure



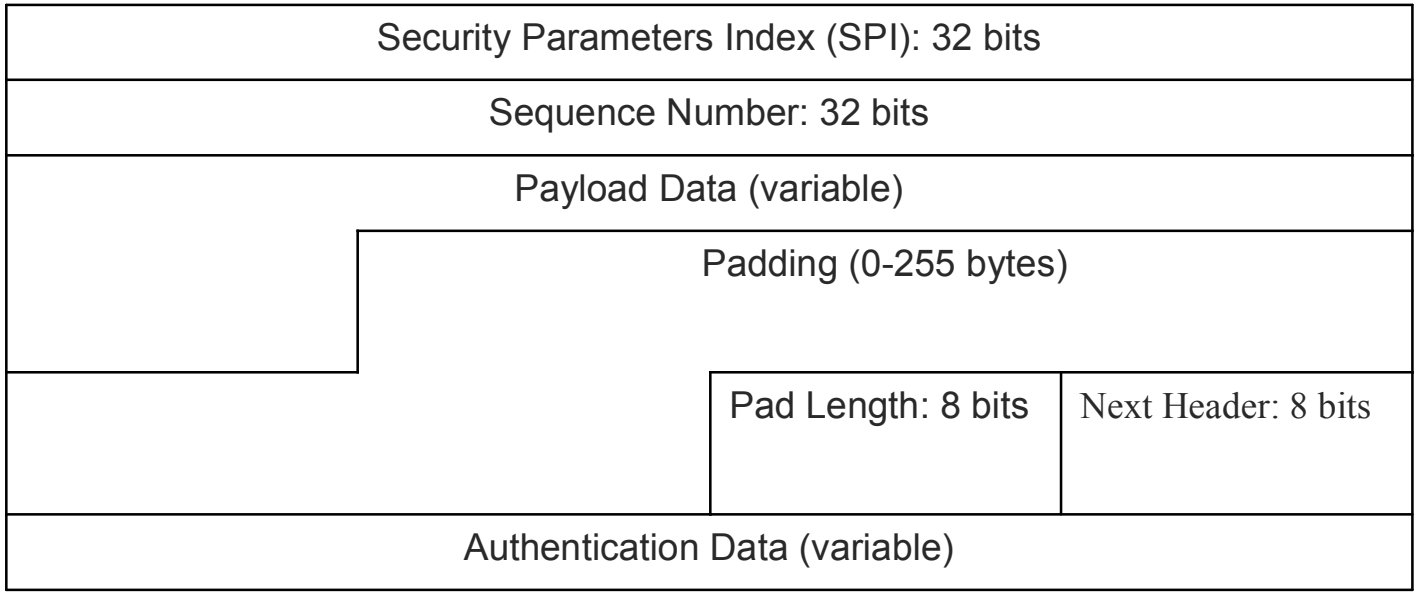
IP Security (IPSec) Background

- The most deployed protocol: IP
- OSI Layer



Protocols in IPSec: ESP and AH

- ESP: Encapsulating Security Payload
  - Privacy (Encryption: AES/3DES/DES)
  - Authenticity (Hash: SHA1/MD5)

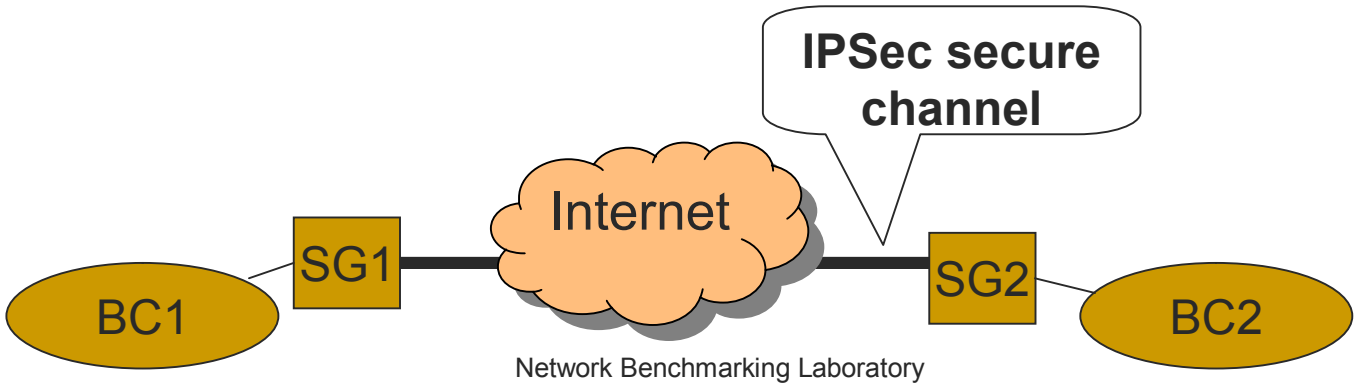


- AH: Authentication Header
  - Authenticity only (Hash: SHA1/MD5)

Next Header: 8 bits	Payload Len: 8 bits	RESERVED: 16 bits
Security Parameters Index (SPI): 32 bits		
Sequence Number Field: 32 bits		
Authentication Data (variable)		

Operation modes in IPSec: Tunnel mode and Transport mode

- Tunnel mode: secure channel for two regions
  - BC1 and BC2 can talk to each other through the IPSec secure channel
  - SG1 and SG2 can NOT do that
- Transport mode: secure channel for two points.
  - SG1 and SG2 can talk to each other through the IPSec secure channel
  - BC1 and BC2 can NOT do that



Security Association (SA) and Security Policy (SP) in IPSec

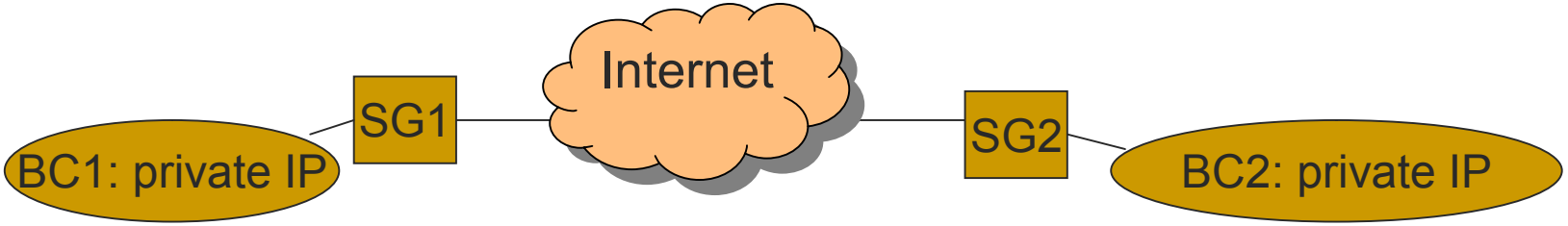
- SA: define what kinds of mechanisms to used to secure those packets
  - Encryption/Hash algorithms
  - Session keys for encryption/hash algorithms
  - Security Parameter Index (SPI)
- SP: define what kinds of packets to be secured
  - Source IP range/Destination IP range
  - ESP or AH
  - Tunnel or Transport
  - Which tunnel to use

Internet Key Exchange (IKE)

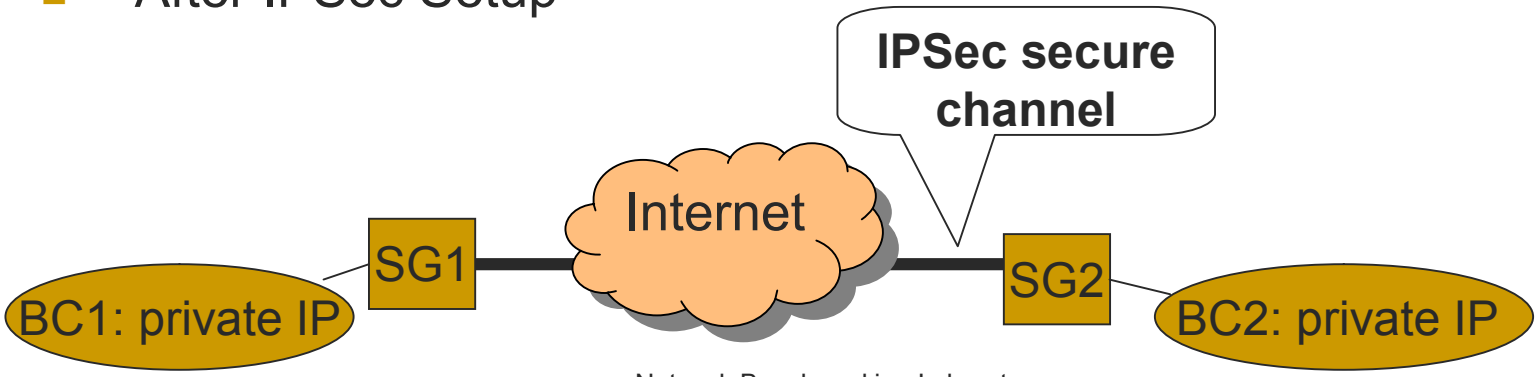
- Automatically install SA in both side of SG.
- Automatically change session keys in a certain time.
- Peer authentication method
  - Certificate
  - Pre-shared key

IPSec VPN Scenario

- Before IPSec Setup



- Assume Pc1 in BC1, Pc2 in BC2
- Pc1 “ping” Pc2 => trigger IKE negotiation => SG1 is initiator, SG2 is responder
- If IKE negotiation successfully => SAs are installed in both SG1 and SG2.
- After IPSec Setup



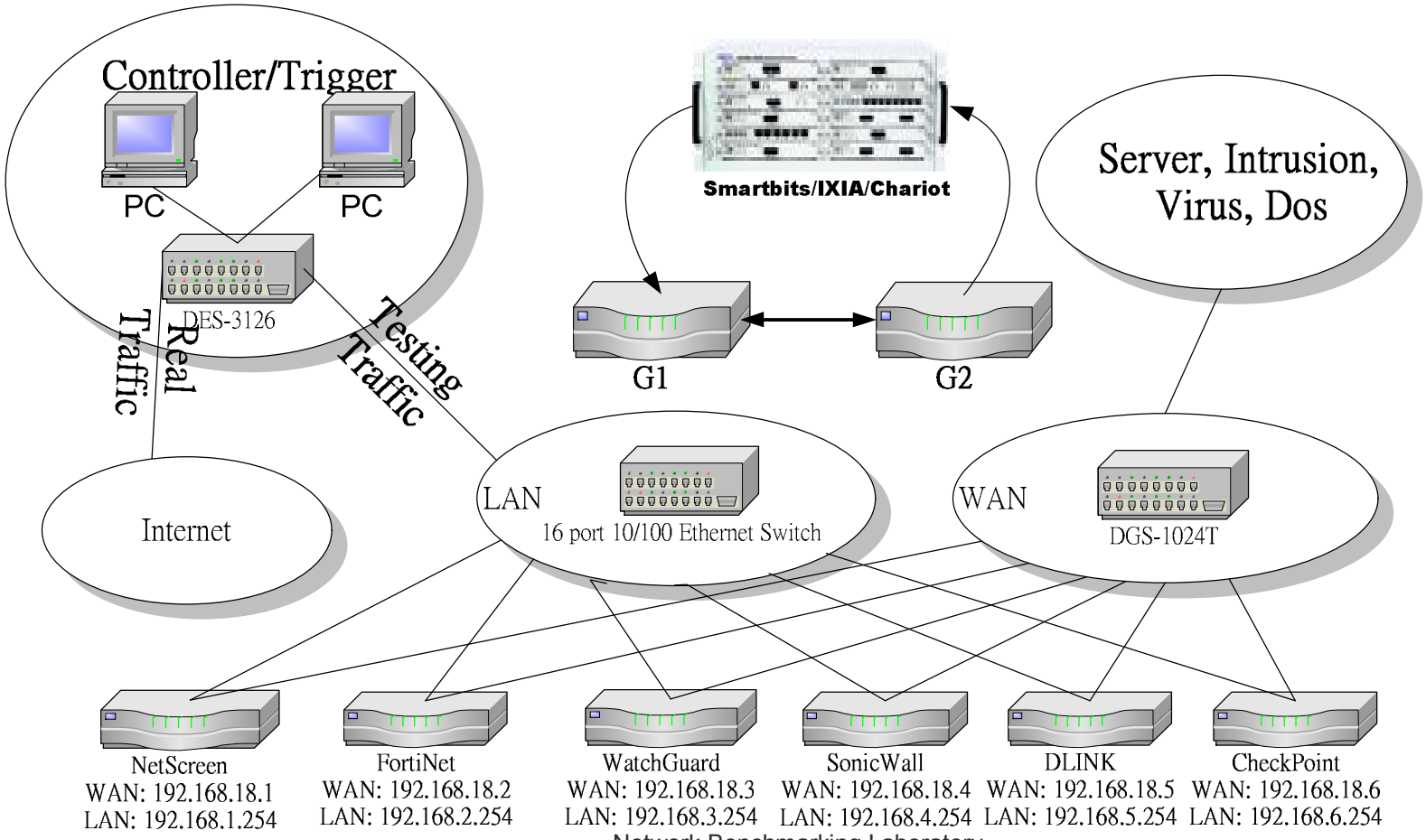
Why IPSec VPN

- Why VPN
- Why IPSec

What're the critical issues in IPSec VPN

- Interoperability (IKE):
  - Too many variables to configure IPSec
  - No "standard" configuration
- Performance
  - Without ASIC, Encryption will greatly slow down the speed of packet processing

TestBed Topology



IPSec Functionality Testing

- Setup two D-Link DFL-900
  - Do NOT enable Firewall function
    - ADVANCED SETTINGS->Firewall-> uncheck “Enable Stateful Inspection Firewall->Apply
  - Enable IPSec VPN
    - ADVANCED SETTINGS->VPN Settings-> IPSec->check Enable IPSec”->Apply
    - Click “IKE” -> Add a proper IPSec rule (Tunnel mode, ESP)
- Use “ping” and “ftp” to setup and pass through the IPSec tunnel
- Collect the Log data
  - DEVICE STATUS->VPN Logs->IPSec Logs
  - Copy to the report

IPSec Interoperability Testing

- Setup one D-Link DFL-900 and another vendor's device
  - NetScreen 5GT
  - Fortinet Fortigate-50
  - Soniwall SOHO-3
  - WatchGuard SOHO-6
  - D-Link DFL-100
- Use "ping" and "ftp" to setup and pass through the IPSec tunnel (Tunnel mode, ESP)
- Collect the IPSec logs which you have done and write a table to describe the Interoperability
- Copy to the Report

IPSec Performance Testing

- Use Smartflow/Smartbits to test the throughput of DFL-900 IPSec
- Variables affecting throughput
  - Null/SHA1, 3DES/SHA1, AES/SHA1
  - Frame size: 64, 512, 1450, 1518 bytes
- Collect the test result from smartflow
  - Results->Export All Tests to File
  - Copy to the Report

SmartFlow Setting (reference only)

Parameter	Value
Cards	
Port	SMB6000 2A1
Port	SMB6000 2A2
Model (SMB6000 2A1, 2A2)	LAN-6101A/3101A
Auto Negotiation (SMB6000 2A1, 2A2)	Force
Speed (SMB6000 2A1, 2A2)	100M
Duplex (SMB6000 2A1, 2A2)	Full
IPv4 Networks	
Port IP Address (SMB6000 2A1)	192.168.1.1
Network (SMB6000 2A1)	192.168.1.0
Gateway (SMB6000 2A1)	192.168.1.254
Subnet Mask (SMB6000 2A1)	255.255.255.0
Port IP Address (SMB6000 2A2)	192.168.2.1
Network (SMB6000 2A2)	192.168.2.0
Gateway (SMB6000 2A2)	192.168.2.254
Subnet Mask (SMB6000 2A2)	255.255.255.0

SmartFlows	
2A1 -> 2A2	
IP's next protocol	NONE/UDP/TCP
IP Source	192.168.2.3
IP Destination	192.168.1.3
Test Setup	
Frame size with CRC (bytes)	64/512/1024/1518
Duration (Sec)	10
Traffic test mode	Binary
Traffic initial rate (%)	10
Traffic Minimum rate (%)	1
Traffic Maximum rate (%)	100
Back off (%)	50
Acceptable frame loss (%)	0