行政院國家科學委員會補助專題研究計畫成果報告

網路安全與頻寬控制閘道器之實作與研究

Implementation and Research of Security and Bandwidth Management Gateways

- 計畫類別: 個別型計畫 整合型計畫
- 計畫編號:NSC 90-2213-E-009-161-
- 執行期間: 2001 年 08 月 01 日至 2002 年 7 月 31 日
- 計畫主持人: 林盈達

共同主持人:

- 計畫參與人員:魏焕雲、梁元彪、張智晴
- 本成果報告包括以下應繳交之附件:

赴國外出差或研習心得報告一份 赴大陸地區出差或研習心得報告一份 出席國際學術會議心得報告及發表之論文各一份 國際合作研究計畫國外研究報告書一份

執行單位: 國立交通大學資訊科學系

中文摘要:

網路安全和頻寬管理對企業而言已經成為 一個重要的議題。本研究著重在整合與安 全及頻寬管理相關的開放性原始碼套件在 單一個閘道器上。各套件彼此的衝突已被 消弭以確保其互通性。其次,這項研究並 從內部及外部量測各功能元件的效能,以 發現更進一步的研究議題。我們也提出了 一個會損失封包的廣域網路下較TCR的方 式節省了 96%的緩衝區空間,及提高 10% 的實質輸送量。最後,我們並提供幾種提 升各元件效能方法的建議。

English abstract:

Network bandwidth security and management have become a critical issue for enterprises. The research focuses on integrating components of open source packages for security and bandwidth management into a single gateway. Conflicts among the packages are resolved to ensure interoperability. Next, this study internally and externally evaluates the performance of each component to identify the problems for future research directions. We also propose a PostACK to shape TCP flows, which saves 96% buffer space but also has 10% goodput improvement against TCP rate control (TCR) lossy [1] under a WAN in our implementation. Finally, several approaches to scale up these software components are suggested to improve the performance.

2. Motivation and introduction

To guarantee the secure operations of an enterprise network, firewalls, virtual private networks (VPN) and intrusion detection systems (IDS), respectively, address the requirement. Originally they were separate devices, but they have been integrated with other services such a network address translation (NAT) as a single security gateway. Besides, bandwidth management is an increasing demand. It is expected to be integrated into the gateway as well. We integrate several open source packages for these purposes into a single gateway. These packages are listed in Table 1 [2-7].

Package Name	User-space Program	Kernel-space Program	Package Size	Version
ipchains	Command-line management tool	Kernel built-in packet filtering firewall and NAT	63KB	1.3.9
Squid	Daemon (Cache server, transparent proxy**, and URL filter)	No	1104KB	2.3
FWTK	Daemon (Application proxies for Web content filter)	No	476KB	2.1
FreeS/WAN	Pluto Daemon (Internet key exchange, IKE)	KLIPS kernel patch (Encryption and authentication)	1252KB	1.5
Snort	Daemon (Intrusion detection)	No	644KB	1.7
ALTO	Management tools	OoS components	507 KB	3.1

Figure 1 illustrates the complete packet processing flows of the security part of the integrated gateway.



Figure 1: Complete Packet Processing Flows of the security Integration

In general, the packet flow from the private interface to the public interface is as follows: (1) perform checksum calculations and sanity checks of the packet; (2) check the packet through the input chain; (3) routes the packet; (4) judge whether the packet is generated by the gateway itself; (5) check the packet through the forward chain; (6) NAT the packet if needed; (7) check the packet through the output chain, and (8) perform VPN processing if needed. In addition, if the packet's source and destination IP addresses both belong to the gateway, i.e., inter-daemon communication from Squid to FWTK, the gateway passes the packet back to the loopback (lo) interface after checking the output chain.

We also propose PostACK to manage TCP traffic. It is designed to be more intelligent both in retaining previous TCR benefits and eliminating its deficiencies. Without measuring the WAN delay and shrinking the RWND in TCP ACKs, PostAck can avoid the side effects of TCR. It has the following advantages: (1) low buffer requirement, (2) low data packet latency, (3) fairness among flows within a class, (4) higher goodput than TCR-applied flows, (5) more robust under various TCP implementations, (6) eliminating triple-dup ACKs. Figure 2 illustrates theis mechanism.



Figure 2: Efficient PostAck implementation for managing outgoing TCP traffic

3. Result and discussion

We perform both internal and external benchmarks to our implementation. Table 2 summarizes the benchmark methodology.

CPU cost SmartFlows SmartBits 2000 with self-written 1.Enable functions all security functions Who tops the processing inclusions Memory and sk cost SmartFlows 1.2, SmartFlows 1.2, self-written Various packet functions Various packet self-written The disk / memory consumptions Packet Filter SmartBits 2000 with SmartFlows 1.2, SmartFlows 1.2 4. 10 URL entries are configured SmartBits 2000 with 1. Only enable packet filter Scalability Packet Filter SmartBits 2000 with SmartFlows 1.2 1. Only enable packet filter Scalability URL Filiter Self-written HTTP Traffic Generator 2. Various numbers of filters Scalability URL Filiter self-written HTTP Traffic Generator 2. Various Web page sizes Scalability Scalability Content Filter HTTP Generator Traffic I SmartFlows 1.2 1. Various web page sizes Scalability Scalability IP SmartFlows 1.2 1. Various numbers of concurrent connections S A single HTTP connection repeatedly retrieves a 64KB Web page for 10 seconds Scalability IP SmartFlows 1.2 for public interface and 3 for private nosts S. Various numbers of private hosts S. Various numbers of private hosts Scalability Authentication Al	Category	Benchmark Tools	Settings	Benchmark Items	
SmartFlows 1.2, self-written functions ipchains processing among all the functions Memory and disk cost SmartBits 2000 with self-written HTTP Traffic Generator 3. Using 3DES / MD5 4. 10 URL entries are configured The disk / memory consumptions Self-written HTTP Traffic Generator 5. A single HTTP connection repeatedly retrieves a 40KB Web The disk / memory consumptions Packet Filter SmartBits 2000 with SmartFlows 1.2 1. Only enable packet filter Scalability URL Filter Self-written HTTP SmartFlows 1.2 1. Various numbers of filters Scalability URL Filter self-written HTTP Traffic Generator 1. Various Web page sizes Scalability URL Filter self-written HTTP Traffic Generator 1. Various Web page sizes Scalability Content Filter HTTP Traffic I 1. Various Web page sizes Scalability Content Filter HTTP Traffic I 2. Various numbers of concurrent connections Scalability IP SmartFlows 1.2 SmartFlows 1.2 Scalability IP SmartFlows 1.2 for private hosts Svarious numbers of private hosts SmartFlows 1.2 for private interfaces 2. Various numbers of private hosts	CPU cost	SmartBits 2000 with	1. Enable all security	Who tops the	
self-written HTTP Traffic Generator 2. No other filters in among all the functions Memory and SmartFlows 1.2, self-written HTTP Traffic Generator 3. Using 3DES / MD5 The disk / memory configured Packet Filter SmartBits 2000 with SmartFlows 1.2 4. 10 URL entries are configured The disk / memory consumptions Packet Filter SmartBits 2000 with SmartFlows 1.2 1. Only enable packet filter Scalability URL Filter SmartBits 2000 with SmartFlows 1.2 1. Only enable packet filter Scalability URL Filter self-written HTTP Traffic Generator 1. Various web page sizes Scalability URL Filter self-written HTTP Traffic Generator 1. Various Web page sizes Scalability URL Filter self-written HTTP Traffic Generator 1. Various Web page sizes Scalability Content Filter HTTP Generator Traffic I. Various Web page sizes Scalability Content Filter HTTP SmartBits 2000 with 1. Security gateway equipped with 4 NICs. 1 for public interface and 3 for private hosts Scalability P SmartBits 2000 with 1. Security gateway Scalability Scalability IP SmartFlows 1.2 Smartous packet sizes Cost of MD5 and SHA1 <td></td> <td>SmartFlows 1.2,</td> <td>functions</td> <td>processing time</td>		SmartFlows 1.2,	functions	processing time	
Traffic Generator ipchains functions Memory and SmartBits 2000 with disk cost 3. Using 3DES / MD5 The disk / memory consumptions SmartFlows 1.2, self-written HTTP Traffic Generator 5. A single HTTP connection repeatedly retrieves a 40KB Web page for 10 seconds Scalability Packet Filter SmartBits 2000 with SmartFlows 1.2 1. Only enable packet filter 3. Various numbers of filter 3. Various numbers of grive a 64KB Web page for 10 seconds Scalability URL Filter self-written HTTP 1. Various Web page sizes 3. A single HTTP connection repeatedly retrieves a 64KB Web page for 10 seconds Scalability Content Filter HTTP Traffic Generator 2. Various numbers of concurrent connections 3. A single HTTP connection repeatedly retrieves a 64KB Web page for 10 seconds Scalability Content Filter HTTP Traffic Generator 2. Various numbers of concurrent connections 3. A single HTTP connection repeatedly retrieves a 64KB Web page for 10 seconds Scalability IP SmartBits 2000 with 1. Security gateway equipped with 4 NICs. 1 for public interface and 3 for private hosts 3. Various numbers of private hosts 3. Vari		self-written HTTP	2. No other filters in	among all the	
Memory and SmartBits 2000 with 3. Using 3DES / MD5 SmartFlows 1.2, self-written HTTP Traffic Generator The disk / memory consumptions Packet Filter SmartBits 2000 with 1. Only enable packet Scalability retrieves a 40KB Web page for 10 seconds Scalability Packet Filter SmartBits 2000 with 1. Only enable packet Scalability filter 2. Various numbers of filters 3. Various packet sizes Scalability URL Filter Self-written HTTP Traffic Generator 1. Various Web page sizes 2. Various numbers of filters 3. Various numbers of concurrent connection repeatedly retrieves a 64KB Web page for 10 seconds Scalability Content Filter HTTP Traffic I. Various Web page sizes 3. A single HTTP connection repeatedly retrieves a 64KB Web page for 10 seconds Scalability Packet Filter HTTP Traffic I. Various Web page sizes 3. A single HTTP connection repeatedly retrieves a 64KB Web page for 10 seconds Scalability IP SmartBits 2000 with 1. Security gateway scalability equipped with 4 NICs. 1 for public interface and 3 for private hosts 3. A rious numbers of private hosts 3. Various packet sizes Cost of MD5 and SHA1 IDS SmartBits 2000 with SmartFlows 1.2 Various packet sizes 2. Patcket los		Traffic Generator	ipchains	functions	
disk cost SmartFlows 1.2, 4. 10 URL entries are consumptions self-written HTTP configured connection repeatedly retrieves a 40KB Web page for 10 seconds Packet Filter SmartBits 2000 with 1. Only enable packet filter Scalability SmartFlows 1.2 filter 2. Various numbers of filters URL Filter self-written HTTP 1. Various Web page sizes Scalability Traffic Generator 2. Various URL lengths in HTTP request 3. A single HTTP connection repeatedly retrieves a 64KB Web page for 10 seconds Content Filter HTTP Traffic Generator 2. Various numbers of concurrent connection repeatedly retrieves a 64KB Web page for 10 seconds Content Filter HTTP Traffic I. Various web page sizes Scalability Quarter of the seconds 2. Various numbers of concurrent connection repeatedly retrieves a 64KB Web page for 10 seconds Scalability RemarkBits 2000 with 1. Security gateway Scalability Scalability Masquerade SmartBits 2000 with 1. Security gateway Scalability Scalability equipped with 4 NICs. 1 for problic interfaces 2. Various numbers of private interfaces 2. Various numbers of private hosts Scalability Masquerade SmartBits 2000 with Various packet sizes Cost of MD5 and SHA1 <td>Memory and</td> <td>SmartBits 2000 with</td> <td>3. Using 3DES / MD5</td> <td>The disk / memory</td>	Memory and	SmartBits 2000 with	3. Using 3DES / MD5	The disk / memory	
self-written HTTP Traffic Generator 5. A single HTTP connection repeatedly retrieves a 40KB Web page for 10 seconds Packet Filter SmartBits 2000 with 1. Only enable packet filter Scalability SmartFlows 1.2 SimartFlows 1.2 Filter Scalability URL Filter self-written HTTP 1. Various numbers of filters Scalability URL Filter self-written HTTP 2. Various URL lengths in HTTP request Scalability Content Filter HTTP Traffic Generator 2. Various Web page sizes Scalability Content Filter HTTP Traffic 1. Various Web page sizes Scalability Generator 2. Various numbers of concurrent connections Scalability Masquerade SmartBits 2000 with 1. Security gateway page for 10 seconds Scalability IP Masquerade SmartFlows 1.2 for public interface and 3 for private hosts 3. Various numbers of private hosts 3. Various packet sizes Cost of MD5 and SHA1 Authentication Algorithms SmartFlows 1.2 Various packet sizes Cost of MD5 and SHA1 IDS SmartFlows 1.2 Various packet sizes 1. Packet loss rate 2. pattern-matching	disk cost	SmartFlows 1.2,	4. 10 URL entries are	consumptions	
Traffic Generator 5. A single HTTP connection repeatedly retrieves a 40KB Web page for 10 seconds Packet Filter SmartBits 2000 with SmartFlows 1.2 1. Only enable packet Straining Straini		self-written HTTP	configured		
connection repeatedly retrieves a 40KB Web page for 10 seconds Packet Filter SmartBits 2000 with SmartFlows 1.2 1. Only enable packet filter Scalability 2. Various numbers of filters 5. Various packet sizes Scalability URL Filter self-written HTTP Traffic Generator 1. Various URL lengths in HTTP request Scalability 2. Various numbers of filters 3. A single HTTP connection repeatedly retrieves a 64KB Web page for 10 seconds Scalability Content Filter HTTP Generator Traffic I. Various Neb page sizes 3. A single HTTP connection repeatedly retrieves a 64KB Web page for 10 seconds Scalability IP Masquerade SmartBits 2000 with 1. Security gateway SmartFlows 1.2 Scalability equipped with 4 NICs. 1 for public interfaces 2. Various numbers of private hosts 3. Various packet sizes Authentication Algorithms SmartBits 2000 with SmartFlows 1.2 Various packet sizes Cost of MD5 and SHA1 IDS SmartFlows 1.2 Various packet sizes 1. Packet loss rate 2. pattern-matching		Traffic Generator	A single HTTP		
Packet Filter SmartBits 2000 with 1. Only enable packet Scalability Packet Filter SmartFlows 1.2 filter 2. Various numbers of filters Surger Self-written HTTP 1. Various Web page sizes Scalability URL Filter self-written HTTP 2. Various URL lengths in HTTP request Traffic Generator 2. Various URL lengths in HTTP request 3. A single HTTP Content Filter HTTP Traffic I. Various web page sizes Scalability Content Filter HTTP Traffic I. Various numbers of concurrent connections Scalability Generator 2. Various numbers of concurrent connections Scalability Masquerade SmartBits 2000 with I. Security gateway gateway scalability equipped with 4 NICs. 1 for provate interfaces and 3 for private interfaces Scalability Masquerade SmartBits 2000 with Various packet sizes Cost of MD5 and SHA1 IDS SmartBits 2000 with Various packet sizes Cost of MD5 and SHA1 Mathematication SmartBits 2000 with Various packet sizes Cost of MD5 and SHA1			connection repeatedly		
page for 10 seconds Packet Filter SmartBits 2000 with 1. Only enable packet Scalability filter SmartFlows 1.2 filter 2. Various numbers of filter 3. Various packet sizes URL Filter self-written Traffic Generator 2. Various Web page sizes Scalability 2. Various URL lengths in HTTP request 3. A single HTTP request 3. A single for 10 seconds Scalability Content Filter HTTP Traffic 1. Various Web page sizes Scalability Content Filter HTTP Traffic 1. Various wubepage sizes Scalability Content Filter HTTP Traffic 1. Various wubepage sizes Scalability Quarter of the seconds 2. Various numbers of concurrent connections 3. A single HTTP connection repeatedly retrieves a 64KB Web page for 10 seconds IP SmartBits 2000 with 1. Security gateway scalability Masquerade SmartFlows 1.2 for public interface and 3 for private hosts 3. Various numbers of private hosts 3. Various numbers of private hosts 3. Various packet sizes Authentication SmartBits 2000 with Various packet sizes Cost of MD5 and SHA1 IDS SmartBits 2000 with Various packet si			retrieves a 40KB Web		
Packet Filter SmartBits 2000 with SmartFlows 1.2 1. Only enable packet Scalability URL Filter self-written HTTP 2. Various numbers of filters 3. Various packet sizes URL Filter self-written HTTP 1. Various Web page sizes Scalability URL Filter self-written HTTP 1. Various Web page sizes Scalability URL Filter self-written HTTP 2. Various URL lengths in HTTP request Scalability 3. A single HTTP concurrent on separatelly retrieves a 64KB Web Web generator 2. Various numbers of concurrent connections Scalability 3. A single HTTP connection repeatedly retrieves a 64KB Web Scalability Querate SmartBits 2000 with 1. Security Scalability IP SmartFlows 1.2 for private hosts 3. Various numbers of private hosts Querate hosts Authentication SmartBits 2000 with Various packet sizes Cost of MD5 and SHA1 IDS SmartBits 2000 with Various packet sizes 1. Packet loss rate 2. pattern-matching			page for 10 seconds		
SmartFlows 1.2 filter 2. Various numbers of filters 3. Various packet sizes URL Filiter self-written HTTP 1. Various URL lengths in HTTP request 3. A single HTTP content Filter HTTP Traffic Generator 2. Various URL lengths in Content Filter HTTP Generator 2. Various web page sizes Content Filter HTTP Traffic Generator 2. Various numbers of concurrent connections 3. A single HTTP Generator 2. Various numbers of concurrent connections 3. A single HTTP connection repeatedly retrieves a 64KB Web page for 10 seconds IP SmartBits 2000 with 1. Security gateway scalability Masquerade SmartFlows 1.2 Authentication SmartBits 2000 with Authentication SmartBits 2000 with Authentication SmartBits 2000 with SmartBits 2000 with Various packet sizes Authentication SmartBits 2000 with SmartBits 2000 with Various packet sizes Authentication SmartBits 2000 with Masing SmartBits 2000 with Various packet sizes Cost of MD5 and SHA1 IDS SmartBits 2000 with	Packet Filter	SmartBits 2000 with	1. Only enable packet	Scalability	
2. Various numbers of filters 3. Various packet sizes URL Filter self-written HTTP 1. Various Web page sizes 2. Various URL lengths in HTTP request 3. A single HTTP constormed for the page for 10 seconds Content Filter HTTP Traffic Generator 2. Various numbers of concurrent connections 3. A single Bernardor 2. Various numbers of concurrent connections 3. A single HTTP concurrent connections 3. A single HTTP concurrent connections 3. A single HTTP condition repeatedly retrieves a 64KB Web page for 10 seconds IP SmartBits 2000 with Masquerade SmartFlows 1.2 for public interface and 3 for private hosts 3. Various packet sizes Authentication Algorithms SmartFlows 1.2		SmartFlows 1.2	filter		
filters filters 3. Various packet sizes 3. Various packet sizes URL Filiter self-written HTTP Traffic Generator 2. Various WtL lengths in HTTP request Scalability 3. A single HTTP content Filter HTTP Traffic Generator 2. Various Web page sizes Scalability Content Filter HTTP Traffic 1. Various Web page sizes Scalability Content Filter HTTP Traffic 1. Various mumbers of concurrent connections Scalability Representation 3. A single HTTP connection repeatedly Scalability IP SmartBits 2000 with 1. Security gateway Scalability Masquerade SmartFlows 1.2 for private hosts 3. Various numbers of private hosts 3. Various packet sizes Authentication SmartBits 2000 with Various packet sizes Cost of MD5 and SHA1 IDS SmartBits 2000 with SmartFlows 1.2 Various packet sizes 1. Packet loss rate 2. pattern-matching			2. Various numbers of		
3. Various packet sizes URL Filiter self-written HTTP 1. Various URL lengths in HTTP request Scalability 2. Various URL lengths in HTTP request HTTP 3. A single HTTP connection repeatedly retrieves a 64KB Web page for 10 seconds Content Filter HTTP HTTP Traffic I. Various web page sizes Content Filter HTTP Generator 2. Various numbers of concurrent connections 3. A single HTTP connection repeatedly retrieves a 64KB Web page for 10 seconds IP SmartBits 2000 with 1. Security gateway for private interfaces Masquerade SmartFlows 1.2 Authentication Algorithms SmartBits 2000 with SmartFlows 1.2 Authentication Algorithms SmartBits 2000 with SmartFlows 1.2 DS SmartBits 2000 with SmartFlows 1.2			filters		
URL Filter self-written HTTP 1. Various Web page sizes Scalability Traffic Generator 2. Various URL lengths in HTTP request 3. A single HTTP Scontent Filter HTTP Traffic 1. Various web page sizes Scalability Content Filter HTTP Traffic 1. Various web page sizes Scalability Content Filter HTTP Traffic 1. Various web page sizes Scalability Generator 2. Various numbers of concurrent connections 3. A single HTTP connection repeatedly retrieves a 64KB Web page for 10 seconds IP SmartBits 2000 with 1. Security gateway equipped with 4 NICs. 1 for public interface and 3 for private hosts 3. Various packet sizes Scalability Authentication SmartBits 2000 with Various packet sizes Cost of MD5 and SHA1 IDS SmartBits 2000 with SmartFlows 1.2 Various packet sizes 1. Packet loss rate 2. pattern-matching			Various packet sizes		
Traffic Generator 2. Various URL lengths in HTTP request 3. A single HTTP connection repeatedly retrieves a 64KB Web Description Traffic I. Various Web page sizes Content Filter HTTP Traffic I. Various Web page sizes Generator 2. Various numbers of concurrent connections 3. A single HTTP Generator 1. Various Web page sizes Scalability 2. Various numbers of concurrent connections 3. A single HTTP connection repeatedly retrieves a 64KB Web page for 10 seconds IP SmartBits 2000 with Masquerade SmartFlows 1.2 for private metherace and for private hosts 3. Various packet sizes Authentication Algorithms SmartBits 2000 with SmartFlows 1.2 DS SmartBits 2000 with SmartFlows 1.2	URL Filiter	self-written HTTP	 Various Web page sizes 	Scalability	
HTTP request 3. A single HTTP Content Filter HTTP Traffic HTTP Traffic Various Web page sizes Content Filter HTTP Traffic Generator 2. Various numbers of concurrent connections 3. A single HTTP connections 3. A single HTTP request Masquerade SmartBits 2000 with SmartFlows 1.2 For public interface and 3 for private interfaces Authentication SmartBits 2000 with Authentication SmartBits 2000 with SmartBits 2000 with Various packet sizes Authentication SmartBits 2000 with SmartBits 2000 with Various packet sizes Authentication SmartBits 2000 with SmartBits 2000 with Various packet sizes Authentication SmartBits 2000 with SmartBits 2000 with Various packet sizes Authentication SmartBits 2000 with SmartBits 2000 with Various packet sizes Cost of MD5 and SHA1 SmartBits 2000 with SmartBits 2000 with Various packet sizes Li Packet loss rate 2. pattern-matching		Traffic Generator	Various URL lengths in		
3. A single HTTP connection repeatedly retrieves a 64KB Web page for 10 seconds Content Filter HTTP Traffic Generator 1. Various Web page sizes 2. Various numbers of concurrent connections 3. A single HTTP connection repeatedly retrieves a 64KB Web page for 10 seconds IP SmartBits 2000 with Masquerade 1. Security gateway smartFlows 1.2 Masquerade SmartBits 2000 with SmartBits 2000 with Algorithms 1. Security gateway for private hosts 3. Various packet sizes Authentication Algorithms SmartBits 2000 with SmartFlows 1.2 Various packet sizes Cost of MD5 and ShartFlows 1.2 Scal of MD5 and SHA1			HTTP request		
Connection repeatedly retrieves a 64KB Web page for 10 seconds Content Filter HTTP Traffic 1. Various Web page sizes Scalability Content Filter HTTP Traffic 1. Various numbers of concurrent connections Scalability 3. A single HTTP connection repeatedly retrieves a 64KB Web page for 10 seconds Scalability IP SmartBits 2000 with 1. Security gateway gation for public interface and for private interfaces Scalability 2. Various numbers of private hosts 3. Various numbers of private hosts StartFlows 1.2 Cost of MD5 and SHA1 IDS SmartBits 2000 with 1.2 Various packet sizes 1. Packet loss rate 2. pattern-matching			A single HTTP		
IP SmartBits 2000 with SmartBits 2000 with Algorithms SmartBits 2000 with SmartFlows 1.2 I. Security For public interfaces Scalability Scalability 1DS SmartBits 2000 with SmartFlows 1.2 SmartBits 2000 with for public interfaces Scalability Scalability 2. Various numbers of concurrent connections 3. A single HTTP connection repeatedly retrieves a 64KB Web page for 10 seconds Scalability 1P SmartBits 2000 with SmartFlows 1.2 1. Security for public interfaces Scalability Scalability Masquerade SmartBits 2000 with SmartFlows 1.2 1. Security for public interfaces Scalability Scalability 1DS SmartFlows 1.2 SmartFlows 1.2 Cost of MD5 and SHA1			connection repeatedly		
page for 10 seconds Content Filter HTTP Traffic 1. Various Web page sizes Scalability Generator 2. Various numbers of concurrent connections 3. A single HTTP connection repeatedly retrieves a 64KB IP SmartBits 2000 with 1. Security gateway Scalability Masquerade SmartFlows 1.2 for public interface and 3 for private hosts S. Various numbers of private hosts Authentication SmartBits 2000 with Various packet sizes Cost of MD5 and SHA1 IDS SmartFlows 1.2 Various packet sizes 1. Packet loss rate 2. pattern-matching			retrieves a 64KB Web		
Content Filter HTTP Traffic 1. Various Web page sizes Scalability Generator 2. Various numbers of concurrent connections 3. A single HTTP concurrent connections 3. A single HTTP Free connections Masquerade SmartBits 2000 with 1. Security gateway Scalability Masquerade SmartFlows 1.2 for pivate hosts 3. Various numbers of private hosts 3. Various packet sizes Authentication SmartBits 2000 with Various packet sizes Cost of MD5 and SHA1 IDS SmartFlows 1.2 Various packet sizes 1. Packet loss rate 2. pattern-matching	-		page for 10 seconds		
Generator 2. Various numbers of concurrent connections 3. A single HTTP connections 3. A single HTTP connections age for 10 seconds page for 10 seconds IP SmartBits 2000 with 1. Security gateway equipped with 4 NICs. 1 for public interface and 3 for private interfaces Scalability Masquerade SmartFlows 1.2 for private interfaces Scalability Authentication SmartBits 2000 with Various packet sizes Authentication SmartBits 2000 with Various packet sizes SHA1 IDS SmartBits 2000 with SmartBits 2000 with SmartBits 1.2 Various packet sizes 1. Packet loss rate 2. pattern-matching	Content Filter	HTTP Traffic	 Various Web page sizes 	Scalability	
Concurrent connections 3. A single HTTP connection repeatedly retrieves a 64KB Web page for 10 seconds IP Masquerade SmartBits 2000 with 1. Security gateway SmartFlows 1.2 Scalability equipped with 4 NICs. 1 for public interface and 3 for private interfaces 2. Various numbers of private hosts Authentication Algorithms SmartBits 2000 with SmartFlows 1.2 Various packet sizes Authentication SmartFlows 1.2 SmartBits 2000 with Various packet sizes Cost of MD5 and SHA1 IDS SmartFlows 1.2 Various packet sizes 1. Packet loss rate 2. pattern-matching		Generator	2. Various numbers of		
3. A single HTTP connection repeatedly retrieves a 64KB Web page for 10 seconds IP SmartBits 2000 with 1. Security gateway SmartFlows 1.2 Masquerade SmartBits 2000 with 1. Security gateway for private hosts 3. Various packet sizes Authentication Algorithms SmartBits 2000 with SmartFlows 1.2 SmartBits 2000 with SmartFlows 1.2 Various packet sizes SmartFlows 1.2 DS SmartFlows 1.2 SmartFlows 1.2 L Packet loss rate 2. pattern-matching			concurrent connections		
Connection repeatedly retrieves a 64KB Web page for 10 seconds IP SmartBits 2000 with SmartFlows 1.2 1. Security equipped with 4 NICs. 1 for public interface and 3 for private interfaces Scalability Authentication SmartBits 2000 with SmartFlows 1.2 Various numbers of private hosts Scalability Authentication SmartBits 2000 with SmartFlows 1.2 Various packet sizes Cost of MD5 and SHA1 IDS SmartFlows 1.2 Various packet sizes 1. Packet loss rate 2. pattern-matching			3. A single HTTP		
retrieves a 64KB Web page for 10 seconds IP SmartBits 2000 with 1. Security gateway Masquerade Scalability Masquerade SmartBits 2000 with 1. Security gateway for public interface and 3 for private interfaces 2. Various numbers of private hosts Scalability Authentication SmartBits 2000 with SmartBits 2000 with Various packet sizes Cost of MD5 and SHA1 IDS SmartFlows 1.2 Various packet sizes 1. Packet loss rate 2. pattern-matching			connection repeatedly		
IP SmartBits 2000 with I. Security gateway Scalability Masquerade SmartFlows 1.2 for public interface and 3 for private hosts Source			retrieves a 64KB Web		
IP SmartBits 2000 with 1. Security gateway Scalability Masquerade SmartFlows 1.2 equipped with 4 NICs. 1 for public interfaces for private interfaces additional security 2. Various numbers of private hosts 3. Various packet sizes Authentication Algorithms SmartFlows 1.2 SHA1 IDS SmartBits 2000 with SmartBits 2000 with SmartFlows 1.2 Various packet sizes 1. Packet loss rate 2. pattern-matching SmartFlows 1.2 Various packet sizes 2. pattern-matching		a	page for 10 seconds	a 1100	
masquerade SmartFlows 1.2 equipped with 4 NICs. 1 for public interface and 3 for private interfaces 2. Various numbers private hosts 2. Various numbers 3. Various packet sizes 6 Authentication SmartBits 2000 with SmartFlows 1.2 Various packet sizes Cost of MD5 and SHA1 IDS SmartBits 2000 with SmartFlows 1.2 Various packet sizes 1. Packet loss rate 2. pattern-matching	IP Maximum	SmartBits 2000 with	1. Security gateway	Scalability	
Ior public interface and 3 for private interfaces Ior public interfaces 2. Various numbers of private hosts 2. Various numbers of private hosts 3. Various packet sizes 2. Various packet sizes Authentication SmartBits 2000 with Various packet sizes Cost of MD5 and SHA1 IDS SmartFlows 1.2 SmartFlows 1.2 Various packet sizes 2. pattern-matching	Masquerade	SmartFlows 1.2	equipped with 4 NICs. 1		
Ior private interfaces 2. Various numbers of private interfaces 2. Various numbers 0 private hosts 3. Various packet sizes Authentication SmartBits 2000 with Various packet sizes Cost of MD5 and Algorithms SmartFlows 1.2 SHA1 SHA1 IDS SmartFlows 1.2 1. Packet loss rate 2. pattern-matching	1		for public interface and 3		
Authentication SmartBits 2000 with SmartFlows 1.2 Various packet sizes Cost of SHA1 IDS SmartBits 2000 with SmartFlows 1.2 Various packet sizes 1. Packet loss rate 2. pattern-matching	1		2 Various numbers		
Bits Description			2. various numbers of		
Authentication SmartBits 2000 with Various packet sizes Cost of MD5 and Algorithms SmartFlows 1.2 SHA1 SHA1 IDS SmartBits 2000 with SmartFlows 1.2 Various packet sizes 1. Packet loss rate 2. pattern-matching			2 Verieus realist sizes		
Adjorithms SmartFlows 1.2 SmartFlows	Authoritoria	SmontDite 2000	J. various packet sizes	Cost of MD5	
IDS SmartBows 1.2 SHA1 SmartBows 1.2 L. Packet loss rate SmartBows 1.2 2. pattern-matching	Autnentication	SmartBits 2000 with	various packet sizes	COST OF MD5 and	
SmartFlows 1.2 2. pattern-matching	Algorithms	SmartDite 2000	Voniono nookot oinoo	3 Dealest loss not:	
Sinarchows 1.2 2. pattern-matching	iDS	SmartBits 2000 with	various packet sizes	1. Packet loss rate	
time a	1	SmartFlows 1.2		2. pattern-matching	

Table 2: Benchmark methodology

Table 3 summarizes the observations of the

benchmark results. It indicates that ipchains and FreeS/WAN are more viable than commercial products, but FWTK and Snort have performance problems.

Module	Characteristics	Bottleneck	Reason	Worst-case Time Complexity
ipchains	CPU-intensive	Increasing the number of filters	Linear matching algorithm	O(<i>l</i> + <i>m</i> + <i>n</i>); <i>l</i> , <i>m</i> , <i>n</i> : number of filters in input, forward, and output chains, respectively
Squid	Memory& CPU-intensive	Increasing the number of URL regular expressions	Linear matching algorithm	O(n(/+m)); /: URL length in HTTP requests; m: average regular expression length; n: number of URL regular expressions
FWTK	CPU-intensive	Increasing the number of HTTP connections and the size of the retrieved Web page	 Parse config file for each request Read only one byte of the Web page from the socket interface at a time 	O(<i>n</i>); <i>n</i> : size of the retrieved Web page
NAT	CPU-intensive	Increasing the number of private-to-public connections	Data structure of NAT table	O(<i>n</i>); <i>n</i> : number of private-to-public connections
FreeS/WAN	CPU-intensive	Using the stronger algorithms	Too many computation for encryption and authentication	O(<i>n</i> * <i>m</i>); m: key length; <i>n</i> . packet size
Snort	CPU-intensive	Packet loss frequently	1. Copy each packet from kernel space to user space 2. Linear matching algorithm	O(<i>I</i> + <i>m</i> * <i>n</i>); <i>I</i> : number of TCP/UDP/ICMP rule tree nodes; <i>m</i> : number of TCP/UDP/ICMP rule options; <i>m</i> : packet size

Table 3: Summary of comparisons

For bandwidth management, we compare the pros and cons of three mechanisms, Per-flow Queuing (PFQ), TCR, and PostAck, as well as their complexity. The results are summarized in Table 4 and 5.

Metrics	PFQ	TCR	PostACK
Goodput (under lossy WAN)	High	Slightly Lower	High
Fairness (fine-grained)	Good	Good Slig	htly Lower
Fairness (under lossy WAN)	Good	Degraded Sim	ilar to PFQ
Buffer Requirement	High	Low	Low
Data Packet Latency	Large	Little	Little
ACK Packet Latency	Little	Little	Large
Robustness (under lossy WAN)	High	Poor	High
Stability (under lossy WAN)	High	Slightly Lower	High

Table 4: Comparison of PFQ, TCR, and POSTACK: performance metrics

Complexity PFQ TCR PostACK				
Classification	per-flow	per-flow	per-flow	
Time	<i>O</i> (1)	<i>O</i> (1)	<i>O</i> (1)	
Space	O(N)	O(N)	O(N)	
RTT Measurement	No	Yes	No	
Header Modification	No	Yes	No	
Checksum Recalculation	No	Yes	No	

Table 5: Comparison of PFQ, TCR, and PostACK: complexity

The following improvements are suggested to scale up the security packages:

(1) Improving the linear-time algorithms

For ipchains, Squid, and Snort, their linear matching algorithms can be accompanied by a flow cache so that active flows can follow a fast path. For example, signature-based IDS such as Snort, most of the signatures (545 of 763 signatures) attack Web servers. By carefully caching the valid URLs, normal URL accesses can bypass the long linear-matching phase of **URL**-related signatures.

(2) Proper implementation tricks

For FWTK, the configuration file should be scanned only once, and the retrieved Web page can be read multiple bytes at once from the kernel space to the user space. For the NAT module, a suitable bucket size for large enterprises can be defined to avoid hash collisions.

(3) Function relocation from daemon to kernel

For some advanced access control policy used in the application proxy, such as FTP, **SMTP** proxy in FWTK, only the control-plane parts are required to be directed to the user-space daemon process for checking. Other data-plane objects should pass directly through the kernel or be blocked, according to the access-control policy. Several works have focused on changing the slow kernel-daemon-kernel data path into a fast kernel data path [8,9,10]. The efforts differ primarily in the flexibility to switch between slow and fast data paths. Numerical results indicate that this pure software-based acceleration of application proxies can improve the performance by a factor of two to four.

(4) Hardware accelerators

For encryption/decryption operations in VPN processing such as that in FreeS/WAN, the 3-DES operations can be offloaded to an accelerator card or ASIC. Typical operations are: (1) formatting the data to be encrypted/decrypted; (2) feeding data to the hardware through programming I/O or DMA channels; (3) waiting for a hardware interrupt to trigger the Interrupt Service Routine (ISR) to check what is happening; (4) finding that the hardware has successfully encrypted/decrypted, and (5) continuing to process the subsequent operations.

(5) PostACK

PostACK can also achieve perfect fairness, as PFQ and TCR can, if the measuring time scale lasts for several RTTs. But if we measure the bandwidth with a very finegrained time scale, PostACK's fairness is slightly degraded. Honestly speaking, ACK control has always been a cool hack, but not a deep solution. Our study provides a big picture of how much we can shape TCP traffic transparently, especially in the lossy WAN environments.

4. Self-evaluation of the result

Integrating many functions into a single all-in-one system or separating them as standalone devices involves security and bandwidth management issues. Manv commercial security gateways choose to be an all-in-one solution. Accordingly, this study focuses only (1) building a product-like all-in-one system from numerous open-source packages and on (2) externally and internally evaluating the performance of such system. However, installing such a device does not mean secured. Other issues, such as correctly setting the administrative policy rules, increasing the security of the network architecture, and increasing the security of the encryption algorithms, are beyond the scope of this study and deserve further attention. The highly integrated system presented here, together with the self-developed Web management console, is downloadable at [11] for hands-on practice.

5. References

[1] S. Karandikar, S. Kalyanaraman, P. Bagal, and B. Packer, *TCP Rate Control*, ACM Computer Communication Review, Vol. 30, No. 1, Jan. 2000.

[2] *ipchains, http://www.netfilter.org/ipchains/.* [3] Squid, http://www.squid-cache.org.

[4] FWTK, http://www.fwtk.org.

[5] FreeS/WAN, http://www.freeswan.org.

[6] Snort, http://www.snort.org.

[7]*ALTQ*,

http://www.csl.sony.co.jp/person/kjc/progra ms.html.

[8] David Maltz, "TCP Splicing for Application Layer Proxy Performance," *IBM Research Report*, March 1998.

[9] Oliver Spatscheck, Jorgen S. Hansen, John H. Hartman, Larry L. Peterson, "Optimizing TCP Forwarder Performance," *IEEE/ACM Transactions on Networking*, Vol.8 No.2, April 2000.

[10] Saibal Kumar Adhya, "Asymmetric TCP Splice: A Kernel Mechanism to Increase the Flexibility of TCP Splice," *Master thesis of Dept. of C.S.*, Indian Institute of Technology, April 2001.

[11] "Integrated security gateway," http://speed.cis.nctu.edu.tw/SG.html.