



-

가

* ** ***

(IPS)
 IPS 가 , IPS 가 가 4
 IPS 가 , IPS
 NSS IPS 가 가 IPS
 가 .



I.

II. IPS

III. IPS 가

IV. IPS 가

V.

I.

(Network-based Intrusion Prevention System: NIPS)

[1].

NIPS

(Intrusion Detection System: IDS)

. NIPS

, 가

* ETRI /
 ** ETRI /
 *** ETRI /

.....

IPS
IPS

IPS가 [2].

- 가 :
- :
- :

NSS IPS IPS 가
[3].

II. IPS

IDS 가 IPS
IPS 가
IPS
(packet dropping) 가 IPS가

(false positive)
IPS
가 가
10 , 36,000 가 , 864,000 가

가 IPS .
IPS , 가 , , , ,
, , , 가 [3].

III. IPS 가

IPS 가 , NSS (test suite) , ,
가 [3]. IPS ,

1. 가

TCP , IPS가
가
가
가
가
가
가
1/4, 1/2, 3/4, . UDP, HTTP
, 1.48 , 20,000

2.

, . NIPS
가 . IPS ,
,
NIPS 가 .
. NIPS가
, 가 . , NSS

.....

[3].

UDP 가 , 500Mbps
HTTP (1Gbps 50%),
가 SYN .

3.

가 IPS .
IPS , 가
가 8 90% , 가
100% , ,
8 ISIC

4.

가.

NIPS 가 ()
() .
IPS 가 (evasion)
가 .
(baseline): , IPS 가 가

- : 19 fragroute
HTTP .
- URL Obfuscation: Whisker 가 URL
obfuscation HTTP .
- : 7 가
FTP , FTP ,
Telnet , RPC fragging.

IPS 가 ,
TCP IPS .

가 , “ ” “ ”
가 .
가 가 ,

(usability) 가 . 가 ,
가 . 가 , IPS
가 .

IV. IPS 가

1.

NSS [3].

- : 100/1,000Mbit

- : Allied Telesyn AT - 9816GB, AT - 9812T
- IPS (,)
- IPS perimeter
-
-
-
- IPS

2.

가.

가 , . 가 가 .

(1)

가 , (Denial of Service: DoS) 가 . , IP . suite 100 . , DNS, DoS, (), , FTP, HTTP, ICMP, reconnaissance, RPC, SSH, Telnet, , 가 CVE(Common Vulnerabilities and Exposures) .

“noisy” 가 “ ” TCP

가 : 가(Attack Recognition Rating: ARR): (disable)

- 가(Attack Block Rating: ABR):

가

가

(default)

가 가

- 가- (ARR-Detect Only: ARRD): /

(%)

- 가- (ARR-Block: ARRB): /

(%)

CVE

48

“

(custom)” ARRD/ARRB 가

가

가

ARRD/ARRB

가

(2)

IPS

, 가

가

가

. IPS

. IPS Evasion

가 가

(evasion)

(1)

, 가

가

(2)

가 IP

(fragmentation)

TCP

(segmentation)

HTTP

-
-
-

가

(3) URL obfuscation

Whisker URL obfuscation
 HTTP . URL , URL ,
 URL, , TAB , case sensitivity, back , splicing.

(4)

Telnet , FTP , FTP
 , (ADMmutate), RPC PROC , RPC
 fragging.

IPS 가

(1) Stateless (Mid-Flows)

Stick Snot 가 (stateless) 가
 . Stick Snot

가
 (session tear down)
 가
 “broken” “ ” 가

(2) ()

가 가 가 가 .

가 가

HTTP

IPS Spirent Avalanche 가 IPS Spirent

Reflector 10,000 1,000,000 TCP HTTP

IPS 가

non-stateful

IPS

가

, IPS

- : 가 가 가

- : 가 가 가 -

- : 가 가 가

(3) ()

가

,

/

가

가

, 가 가

.....

가

가 , 가 가
가 , IPS
250Mbps, 500Mbps, 750Mbps 1,000Mbps

- : ABR
- (Attack Detection Rate: ADR): ADR
, IPS 가
100% ABR 100%

ADR

(1)

UDP

IPS , 가
250Mbps, 500Mbps, 750Mbps 1,000Mbps
가
- 64 - 1,480,000 : 1,500,000
64 “ ”
가
- 440 - 260,000 :
,
가

- 1,514 - 81,720 : 64

- 50,000 : ,
 , IPS .
 - 10,000 - 440 - 280,000 -10
 - 100,000 : 가 ,
 IPS , .

(4)

가 가 HTTP
 , 가
 가 .
 , “ (normal)”
 가 .
 - 72% HTTP (560) + 20% FTP + 6% UDP (256
) 380 - 555 - 22,000 -
 136 , , 가
 . 250Mbps, 500Mbps, 750Mbps 1,000Mbps

(5) “ ”

가 가 가
 가 가 950Mbps
 , -
 , Avalanche
 25 가 , 가
 , (bursty)
 가 , 250Mbps, 500Mbps, 750Mbps 1000Mbps

- HTTP (): 100
 - 25 - 1,000 - 110,000 .

가 HTTP , , “ ”

IPS

- (72% HTTP + 20% FTP + 6% UDP (256
)): 550 - 900 - 130,000

- 11,000 . FTP UDP , ,
 가 ,

“ ” IPS

IPS 가 가

(1)

IPS

, , 가 ,
 가 ,
 - 가

250Mbps 1Gbps , 250Mbps
 IP 가 가 (64 ,
 440 , 1,518) UDP
 가

- :

- 가 : IPS HTTP
 50%
 , 500Mbps- 2,500 - 540 -

.....

115,000 (64 , 440 , 1,514)
) 250Mbps (125Mbps)
 .
 - : 10% DOS/DDOS
 (100Mbps). (64 , 440 ,
 1,514) 250 Mbps (125Mbps) ,

(2)

HTTP , 가가 가
 가
 - : 50% HTTP
 500 Mbps- 2,500
 - 540 - 115,000 ,
 가 .
 - : IPS 가 ,
 10% DOS/DDOS (100Mbps). IPS 가
 ,
 가 .

- IPS 가 가
 가
 - :
 가 8
 100Mbps . 50,000 , 120~350

가 , 100% 가
 /
 가 IPS
 가
 :
 , 100%
 /
 IPS
 가

- ISIC/ESIC/TCPSIC/UDPSIC/ICMPSIC:

ISIC

350Mbps

60,000

690

/

(1)

IDS/IPS

가

- ISIC/ESIC/TCPSIC/UDPSIC/ICMPSIC:

ISIC

350Mbps

60,000

690

.....

. / . , (a)
. (b)
/ . ISIC

V.

, IPS

[4]. IPS 가가 .
, IPS . 2003 ,
, 50
, 200 , 67% IPS

[5].

가 가 ,
가 IPS 가
NSS

[3]. NSS IPS 가

가

,

가

IPS

가

가

< >

[1] , , , “ , ” 1098 , 2003. 6. 3.

[2] Pete Lindstrom, Intrusion Prevention Systems(IPS): Next Generation Firewalls, A Spire Research Report, Spire Security, Mar. 2004.

[3] An NSS Group Report V 1.0, Intrusion Prevention Systems(IPS), Group Test, NSS, Jan., 2004.

[4] , , , “ , ”
1149 , 2004. 6. 9, pp13-24.

[5] , IPS, 가 가, 21C, 2003 8 .