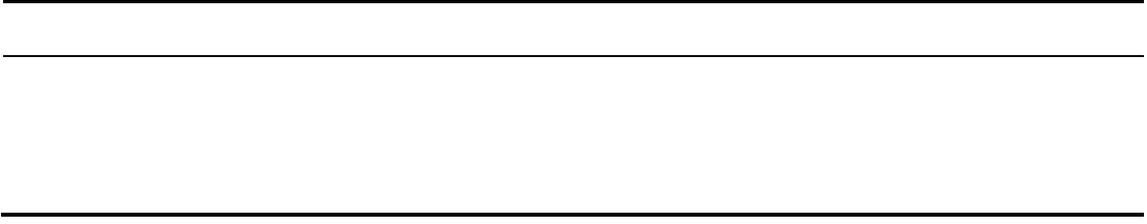

NSF-PROD-NIPS- -

V1.0

V1.0

2017-11-03



		1
		2
2.1		2
2.2		3
2.3	&	4
2.3.1		4
2.3.2		4
2.3.3		4
2.3.4		4
2.3.5	IPv6	5
2.3.6		5
2.3.7	2~7	7
2.3.8	APT	8
2.3.9	Web	9
2.3.10		9
2.3.11		10
2.3.12		10
2.3.13		10
2.3.14		11
2.3.15		12
2.3.16		12
2.3.17		14
2.3.18		14
2.3.19		14
2.3.20		15
2.3.21		15
2.3.22	100G+ NIPS	15
2.4		15
2.5		16
2.5.1		17
2.5.2		18
		19
		20

2.1	3
2.2 NSFOCUS NIPS	17
2.3 NSFOCUS NIPS	18

■

HTTP

DDoS

web2.0

P2P

IM

" NSFOCUS NIPS"

2.3

NSFOCUS NIPS

NSFOCUS NIPS

2.3.1

hIP

NSFOCUS NIPS

2.3.2

NSFOCUS NIPS

NIPS

IP

IP

NSFOCUS NIPS

2.3.3

QQ MSN

Web

P2P

NSFOCUS NIPS

WEB

What When How

“ ”

NSFOCUS NIPS

2.3.5 IPv6

(dual stack)

IPv6/IPv4

IPv4 IPv6

IPv6

IPv6

IPv6

IPv6

NSFOCUS NIPS

IPv6 Ready



IPv6

2.3.6

NSFOCUS NIPS

Smart Tunnel

P2P

P2P

IP

IMS

MSN

NSFOCUS NIPS

NSFOCUS NIPS

RFC

RFC

NSFOCUS NIPS

100%

0

baseline

NSFOCUS NIPS

NSFOCUS NIPS

NSFOCUS NIPS

(DDOS)

2.3.7 2~7

MAPP Microsoft Active Protections Program

NSFOCUS

40

Microsoft HP

CISCO SUN Juniper

NSFOCUS NIPS

3000

NSFOCUS

CVE

CVE

CVE Compatible



NSFOCUS NIPS
SQL

NSFOCUS NIPS

IT

IP **TCP**

NSFOCUS NIPS

IP

TCP

NSFOCUS NIPS

"

"

D.o.S

NSFOCUS NIPS

ICMP Flood

UDP Flood

ACK Flood

D.o.S

D.o.S

2.3.8 APT

APT

IPS

TAC

0day

IPS TAC

IPS

APT

2.3.9

IP

C&C

URL

1.

2. NTI

+

+

3. NTI

NTI

NIPS

1

2 APT

3 24

2.3.10 Web

HTTP

Web

NSFOCUS NIPS

Web

Web

URL

Web

2.3.11

NSFOCUS NIPS

2.3.12

2.3.13

NSFOCUS NIPS

/

/

2.3.15

Web

NSFOCUS NIPS Web IP
MS IE Netscape Firefox Opera

NSFOCUS NIPS

NSFOCUS NIPS

NIPS N

2.3.16

NSFOCUS NIPS

NSFOCUS NIPS

10

MS Word Html JPG

" "

NSFOCUS NIPS

2.3.17

HA

NSFOCUS NIPS

HA

A/A A/S

BYPASS

IPS

,

BYPASS

NSFOCUS NIPS BYPASS

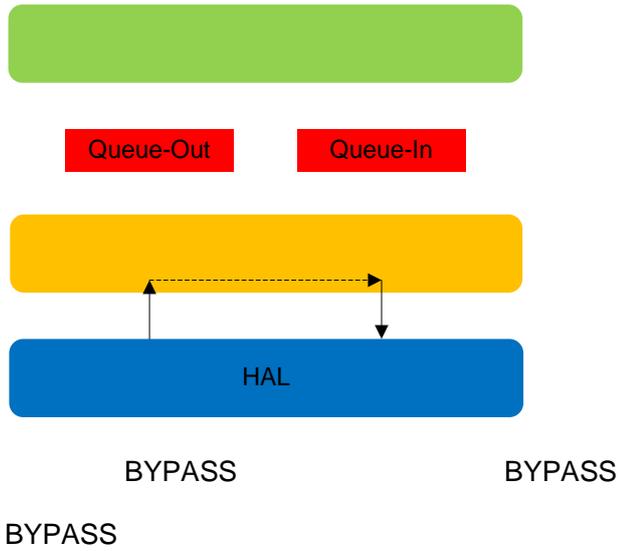
BYPASS

BYPASS IPS

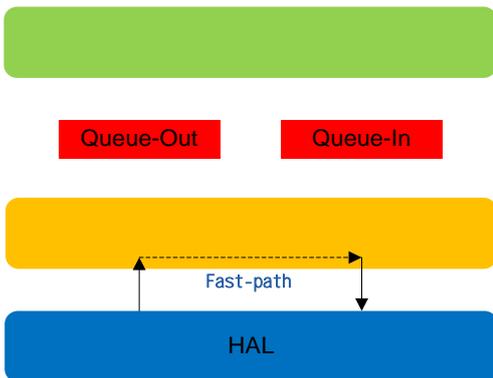
BYPASS

BYPASS

BYPASS



IPS



NSFOCUS NIPS

2.3.21

CPU/

2.5.1

2.5.2

1. NSFOCUS NIPS
2. NSFOCUS NIPS
NIPS N NIPS N
3. NSFOCUS NIPS
4. NIPS N

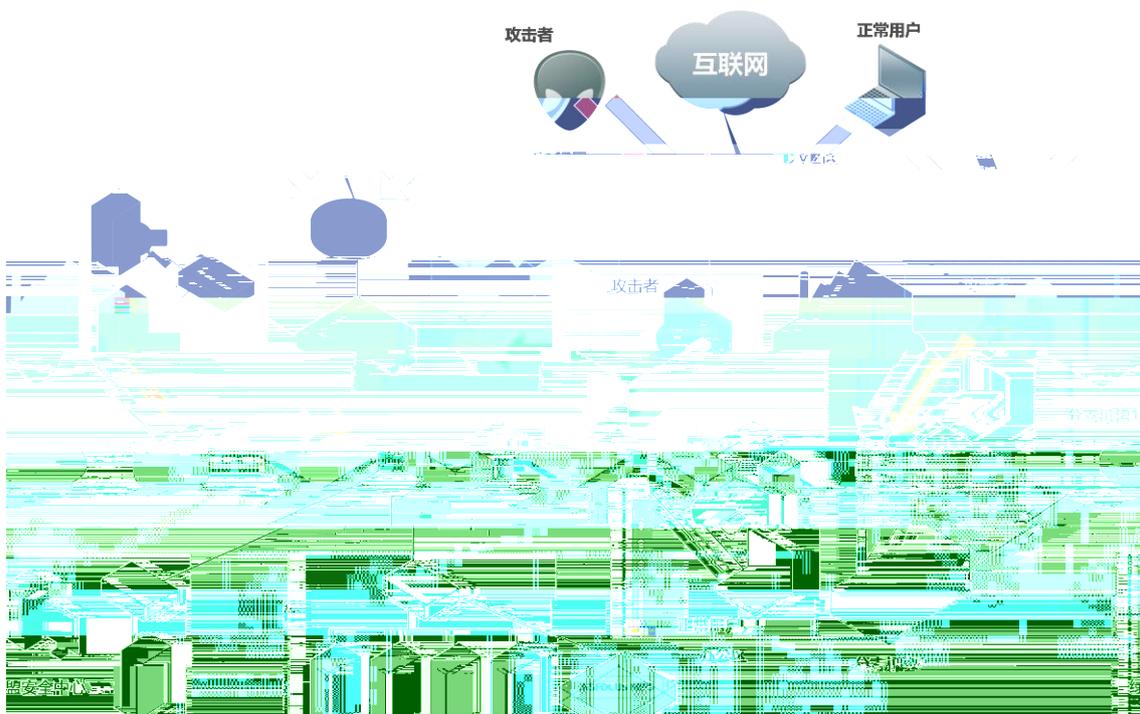


图 2.3 NSFOCUS NIPS

▪

1	Internet				
2	Web	SQL	XSS		
3					DDoS
1					
2					
3					
4					
1					
2					
3					
4					

1

2

3

■

100%

BT P2P
QQ MSN