Frequently Asked Questions

Question

0 I 8 B 0 < 0 @ H @ C B 8 7 0 B > @ 0 Cisco > B DoS 0 B 0 :

Answer

5 7 N < 5 A B 0 B L 8 http://www.informit.com/articles/article.asp?p=345618

8 0 3 = > A B 8 : 0:
F 5 = : 0 7 0 3 @ C 7 : 8 CPU

```
show processes cpu
show processes cpu history
sh int switching
```

! ; 5 6 5 = 8 O 7 0 A G 5 B G 8 : 0 < 8 = 0 ACL

```
clear access-list counters N
show access-list N
```

! 1 @ > A A B 0 B 8 A B 8 : 8 A @ 0 1 0 B K 2 0 = 8 9 ACL 2 syslog:

```
access-list 100 deny icmp any any echo reply log-input
```

Netflow

```
interface N
   ip route-cache flow   8 ; 8 ip route-cache distributed
ip flow-export IP UDP_port
show ip cache flow
Code Red Worms
    show ip cache flow | include 0050
Smurf Attacks
    show ip cache flow | include 0000
clear ip flow stats

TCP SYN Flood Attacks
 access-list 100 tcp permit tcp any any
```

```
ip tcp intercept list 100
ip tcp intercept mode {intercept | watch}
ip tcp intercept watch-timeout {seconds}
ip tcp intercept finrst-timeout {seconds}
ip tcp intercept connection-timeout {seconds}
ip tcp intercept max-incomplete high {N}
ip tcp intercept max-incomplete low {N}
ip tcp intercept drop-mode {oldest | random}
show tcp intercept statistics
show tcp intercept connections
debug ip tcp intercept
```

0 I 8 B 0:

Cisco Express Forwarding (CEF) Switching:

```
scheduler interval Num_of_milliseconds
scheduler allocate Num_of_milliseconds_of_interrupts
Num_of_milliseconds_of_no_interrupts
```

TCP SYN Flood Attacks

! 8 = B 0 : A 8 A

```
access-list N tcp permit tcp any any
ip tcp intercept list N
ip tcp intercept mode {intercept | watch}
ip tcp intercept watch-timeout {seconds}
ip tcp intercept finrst-timeout {seconds}
ip tcp intercept connection-timeout {seconds}
ip tcp intercept max-incomplete high {N}
ip tcp intercept max-incomplete low {N}
ip tcp intercept drop-mode {oldest | random}
show tcp intercept statistics
show tcp intercept connections
debug ip tcp intercept
```

@ 8 < 5 @:

```
access-list 100 tcp permit tcp any host 192.1.1.1 eq 80
access-list 100 tcp permit tcp any host 192.1.1.2 eq 25
ip tcp intercept list 100
```

```
ip tcp intercept mode watch
ip tcp intercept watch-timeout 20
ip tcp intercept connection-timeout 120
ip tcp intercept max-incomplete high 600
ip tcp intercept min-incomplete low 500
ip tcp intercept one-minute high 800
ip tcp intercept one-minute low 600
```

CBAC (Context-Based Access Control) 8 DoS 0 B 0 : 8
! 8 = B 0 : A 8 A:

```
ip inspect tcp synwait-time {seconds}
ip inspect tcp finwait-time {seconds}
ip inspect tcp idle-time {seconds}
ip inspect udp idle-time {seconds}
ip inspect dns-timeout {seconds}
ip inspect max-incomplete high {number}
ip inspect max-incomplete low {number}
ip inspect one-minute high {number}
ip inspect one-minute low {number}
ip inspect tcp max-incomplete host {number} block-time {minutes}
```

@ 8 < 5 @:

```
ip inspect tcp synwait-time 20
ip inspect tcp idle-time 60
ip inspect udp idle-time 20
ip inspect max-incomplete high 400
ip inspect max-incomplete low 300
ip inspect one-minute high 600
ip inspect one-minute low 500
ip inspect tcp max-incomplete host 300 block-time 0
```

Rate Limit:

```
interface N
    no ip unreachables
```

ip icmp rate-limit unreachable [df] {milliseconds}
0 ? @ 8 < 5 @: ip icmp rate-limit unreachable 1000

interface N

rate-limit {input | output} [access-group [rate-limit] acl-index] {bps} {burst_normal}

{burst_max} conform-action {action} exceed-action {action}

@ 8 < 5 @ 1:

```
       interface serial0
           rate-limit output access-group 100 64000 4000 4000
conform-action transmit exceed-action drop
      access-list 100 permit icmp any any echo
      access-list 100 permit icmp any any echo-reply
```

@ 8 < 5 @ 2:

```
      access-list 100 permit tcp any host eq www established
      access-list 101 permit tcp any host eq www
      interface serial0
          rate-limit output access-group 100 1544000 64000 64000
                        conform-action transmit exceed-action drop
          rate-limit output access-group 101 64000 16000 16000
                        conform-action transmit exceed-action drop
```

5 ; > G 8:

```
      no ip directed-broadcast
       no service tcp-small-servers
       no service udp small-servers
```

Details

Info Sunday 14 March 2010 - 18:54:10 by