Chapter 22

NBAR

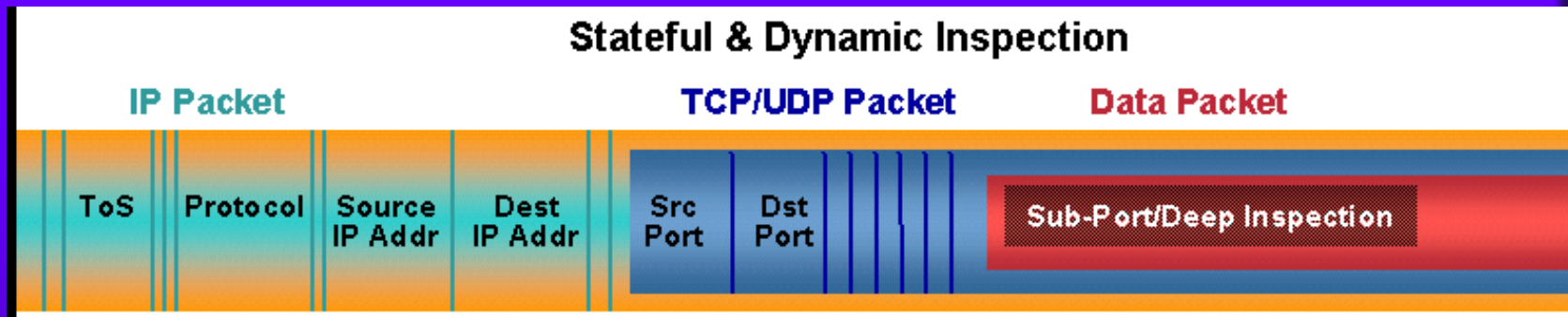
NBAR

- Network-Based Application Recognition
- Available in Cisco IOS
- Monitors traffic at layers 4 through 7
- Can be used to provide QOS to time-sensitive applications
- Can be used to do traffic shaping or bandwidth management
- Can be used to identify and control attacks

Classification of Traffic

- static TCP or UDP port number
- Dynamic TCP or UDP port number
- Non-TCP and non-UDP IP traffic
- Deep packet inspection
- Differentiates approximately 100 protocols and applications

NBAR Packet Inspection



egp	exchange	kerberos	secure-nntp	smtp
gre	finger	l2tp	notes	snmp
icmp	ftp	ldap	novadigm	socks
ipinip	secure-ftp	secure-ldap	ntp	sqlnet
ipsec	gopher	netshow	pcanywhere	ssh
eigrp	http	pptp	pop3	streamwork
bgp	secure-http	sqlserver	secure-pop3	syslog
cuseeme	imap	netbios	printer	telnet
dhcp	irc	nfs	realaudio	secure-telent
dns	secure-irc	nntp	rcmd	tftp
		citrix	napster	vdolive
				xwindows

Supported protocols as of Cisco IOS Software Release 12.2(8)T:

www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/dtnbarad.htm - 1031614

Using NBAR

- Define a traffic class using “class-map”
- Create a traffic policy for class using “policy-map”
- Apply traffic policy to network interface using “service-policy”

NBAR configuration on IOS router to block Code Red Worm

```
class-map match-any codered
    match protocol http url “*default.ida*”
    match protocol http url “*cmd.exe*”
    match protocol http url “*root.exe”

policy-map mark-codered
    class codered
    set ip dscp 1

int serial0
    service-policy input mark-codered

int ethernet0
    ip access-group 100 out

access-list 100 deny ip any any dscp 1
access-list 100 permit ip any any
```

NBAR configuration on IOS router to block Kazaa traffic

```
class-map match-any p2p
    match protocol fasttrack file-transfer *

policy-map block-p2p
    class p2p
        set ip dscp 1

int FastEthernet0
    description PIX/Inside facing interface
    service-policy input block-p2p

int Serial0
    description Internet/Outside facing interface
    ip access-group 100 out

access-list 100 deny ip any any dscp 1
access-list 100 permit ip any any
```