Автор: Administrator
16.03.10 16:23 - Последнее обновление 29.03.10 09:36

Утилиты просмотра, прохождения пакетов, iftop ....

Проверке работоспособности сети:

iftop
iptraf
ntop
tcpdump

При решении проблем с любыми программами в консоли полезно использовать команды:

netstat -it - список интерфейсов, с объемом трафика на каждом, количеством ошибок, коллизий, значением watchdog-таймера
iptstate
ifstat

ifconfig -a покажет настройки сетевых интерфесов.

route или **route -n** - покажет ваши маршруты.

Если нужно прописать маршруты делаем это так
Маршрут для конкретного ip
route add -host 195.26.30.2 gw ваш_второй_шлюз dev eth4

route add -host 172.16.11.4 gw ваш_второй_шлюз dev eth4

Маршрут для подсети.
route add -net 192.168.0.0 netmask 255.255.0.0 gw ваш_второй_шлюз dev eth4
route add -net 172.16.0.0 netmask 255.255.0.0 gw ваш_второй_шлюз dev eth4

Смена шлюза по умолчанию
route del default
route add default gw ваш_второй_шлюз dev eth4
Удалить маршрут
route del 192.168.0.0

Для просмотра цепочек **iptables**, есть много способов вот часть из них.
iptables -nL
iptables -vnL
iptables -t nat -nL
iptables -t filter -nL FORWARD
iptables -t nat -nL POSTROUTING

И вариантов могу перечислить много, но лучше по вкуривать мануал **iptables**. Хотя я знаю, где то его 15 %.
Также нужно понять, при использовании Траффпро. Если включен параметр **control_eth_addr=true**
, то цепочки
INPUT
и
OUTPUT
на сервере ставяться в
DROP
. При включении этого параметра, будьте внимательны.

Для обноления таблиц используйте
iptables -F
iptables -t nat -F
iptables -t mangle -F

После настройки траффпро и обкатки работы, воспользуйтесь командами **tcpdump**, **pi**

ng
и
traceroute

tcpdump -i eth0 dst host
tcpdump -i eth1 src host
tcpdump -i eth1 port ! 22
tcpdump -i eth1 host ! gateway

Это минимум примера для просмотра как у вас проходят пакеты через шлюз.

Это должно помочь новичкам в использовании консоли.
Также полезно просматривать man имя_команды

tcpdump -i eth1 ip broadcast - покажет те компьютеры в сети, кто шлет много пакетов broadcast
tcpdump -i eth1 net 192.168.1.0/24 - покажет какие запросы и куда, из локальной сети.

tcpdump -i eth1 -n ip proto 17 Где proto, это смотреть в /etc/protocols

```
        ip   0 IP   # internet protocol, pseudo protocol number
hopopt  0 HOPOPT   # hop-by-hop options for ipv6
icmp   1 ICMP   # internet control message protocol
igmp   2 IGMP   # internet group management protocol
ggp 3 GGP # gateway-gateway protocol
ipencap 4 IP-ENCAP   # IP encapsulated in IP (officially ``IP'')
st   5 ST   # ST datagram mode
tcp 6 TCP # transmission control protocol
cbt 7 CBT # CBT, Tony Ballardie <A.Ballardie@cs.ucl.ac.uk>
egp 8 EGP # exterior gateway protocol
igp 9 IGP # any private interior gateway (Cisco: for IGRP)
bbn-rcc 10   BBN-RCC-MON # BBN RCC Monitoring
nvp 11   NVP-II   # Network Voice Protocol
pup 12   PUP # PARC universal packet protocol
```

argus 13 ARGUS # ARGUS
emcon 14 EMCON # EMCON
xnet 15 XNET # Cross Net Debugger
chaos 16 CHAOS # Chaos
udp 17 UDP # user datagram protocol
mux 18 MUX # Multiplexing protocol
dcn 19 DCN-MEAS # DCN Measurement Subsystems
hmp 20 HMP # host monitoring protocol
prm 21 PRM # packet radio measurement protocol
xns-idp 22 XNS-IDP # Xerox NS IDP
trunk-1 23 TRUNK-1 # Trunk-1
trunk-2 24 TRUNK-2 # Trunk-2
leaf-1 25 LEAF-1 # Leaf-1
leaf-2 26 LEAF-2 # Leaf-2
rdp 27 RDP # "reliable datagram" protocol
irtp 28 IRTP # Internet Reliable Transaction Protocol
iso-tp4 29 ISO-TP4 # ISO Transport Protocol Class 4
netblt 30 NETBLT # Bulk Data Transfer Protocol
mfe-nsp 31 MFE-NSP # MFE Network Services Protocol
merit-inp 32 MERIT-INP # MERIT Internodal Protocol
dccp 33 DCCP # Datagram Congestion Control Protocol
3pc 34 3PC # Third Party Connect Protocol
idpr 35 IDPR # Inter-Domain Policy Routing Protocol
xtp 36 XTP # Xpress Tranfer Protocol
ddp 37 DDP # Datagram Delivery Protocol
idpr-cmtp 38 IDPR-CMTP # IDPR Control Message Transport Proto
tp++ 39 TP++ # TP++ Transport Protocol
tp++ 39 TP++ # TP++ Transport Protocol
il 40 IL # IL Transport Protocol
ipv6 41 IPv6 # IPv6
sdrp 42 SDRP # Source Demand Routing Protocol
ipv6-route 43 IPv6-Route # Routing Header for IPv6
ipv6-frag 44 IPv6-Frag # Fragment Header for IPv6
idrp 45 IDRP # Inter-Domain Routing Protocol
rsvp 46 RSVP # Resource ReSerVation Protocol
gre 47 GRE # Generic Routing Encapsulation
dsr 48 DSR # Dynamic Source Routing Protocol
bna 49 BNA # BNA
esp 50 ESP # Encap Security Payload
ipv6-crypt 50 IPv6-Crypt # Encryption Header for IPv6 (not in official list)
ah 51 AH # Authentication Header
ipv6-auth 51 IPv6-Auth # Authentication Header for IPv6 (not in official list)
i-nlsp 52 I-NLSP # Integrated Net Layer Security TUBA
swipe 53 SWIPE # IP with Encryption
narp 54 NARP # NBMA Address Resolution Protocol
mobile 55 MOBILE # IP Mobility

tlsp 56 TLSP # Transport Layer Security Protocol
skip 57 SKIP # SKIP
ipv6-icmp 58 IPv6-ICMP # ICMP for IPv6
ipv6-nonxt 59 IPv6-NoNxt # No Next Header for IPv6
ipv6-opts 60 IPv6-Opts # Destination Options for IPv6
61 # any host internal protocol
cftp 62 CFTP # CFTP
63 # any local network
sat-expak 64 SAT-EXPAK # SATNET and Backroom EXPAK
kryptolan 65 KRYPTOLAN # Kryptolan
rvd 66 RVD # MIT Remote Virtual Disk Protocol
ippc 67 IPPC # Internet Pluribus Packet Core
68 # any distributed file system
sat-mon 69 SAT-MON # SATNET Monitoring
visa 70 VISA # VISA Protocol
ipcv 71 IPCV # Internet Packet Core Utility
cpnx 72 CPNX # Computer Protocol Network Executive
cphb 73 CPHB # Computer Protocol Heart Beat
wsn 74 WSN # Wang Span Network
pvp 75 PVP # Packet Video Protocol
br-sat-mon 76 BR-SAT-MON # Backroom SATNET Monitoring
sun-nd 77 SUN-ND # SUN ND PROTOCOL-Temporary
wb-mon 78 WB-MON # WIDEBAND Monitoring
wb-expak 79 WB-EXPAK # WIDEBAND EXPAK
iso-ip 80 ISO-IP # ISO Internet Protocol
vmtp 81 VMTP # Versatile Message Transport
secure-vmtp 82 SECURE-VMTP # SECURE-VMTP
vines 83 VINES # VINES
ttp 84 TTP # TTP
nsfnet-igp 85 NSFNET-IGP # NSFNET-IGP
dgp 86 DGP # Dissimilar Gateway Protocol
tcf 87 TCF # TCF
eigrp 88 EIGRP # Enhanced Interior Routing Protocol (Cisco)
ospf 89 OSPFIGP # Open Shortest Path First IGP
sprite-rpc 90 Sprite-RPC # Sprite RPC Protocol
larp 91 LARP # Locus Address Resolution Protocol
mtp 92 MTP # Multicast Transport Protocol
ax.25 93 AX.25 # AX.25 Frames
ipip 94 IPIP # Yet Another IP encapsulation
micp 95 MICP # Mobile Internetworking Control Pro.
scc-sp 96 SCC-SP # Semaphore Communications Sec. Pro.
etherip 97 ETHERIP # Ethernet-within-IP Encapsulation
encap 98 ENCAP # Yet Another IP encapsulation
99 # any private encryption scheme
gmtp 100 GMTP # GMTP
ifmp 101 IFMP # Ipsilon Flow Management Protocol

pnni 102 PNNI # PNNI over IP
pim 103 PIM # Protocol Independent Multicast
aris 104 ARIS # ARIS
scps 105 SCPS # SCPS
qnx 106 QNX # QNX
a/n 107 A/N # Active Networks
ipcomp 108 IPComp # IP Payload Compression Protocol
snp 109 SNP # Sitara Networks Protocol
compaq-peer 110 Compaq-Peer # Compaq Peer Protocol
ipx-in-ip 111 IPX-in-IP # IPX in IP
vrrp 112 VRRP # Virtual Router Redundancy Protocol
pgm 113 PGM # PGM Reliable Transport Protocol
114 # any 0-hop protocol
l2tp 115 L2TP # Layer Two Tunneling Protocol
ddx 116 DDX # D-II Data Exchange
iatp 117 IATP # Interactive Agent Transfer Protocol
stp 118 STP # Schedule Transfer
srp 119 SRP # SpectraLink Radio Protocol
uti 120 UTI # UTI
smp 121 SMP # Simple Message Protocol
sm 122 SM # SM
ptp 123 PTP # Performance Transparency Protocol
isis 124 ISIS # ISIS over IPv4
fire 125 FIRE
crtp 126 CRTP # Combat Radio Transport Protocol
crdup 127 CRUDP # Combat Radio User Datagram
sscopmce 128 SSCOPMCE
iplt 129 IPLT
sps 130 SPS # Secure Packet Shield
pipe 131 PIPE # Private IP Encapsulation within IP
sctp 132 SCTP # Stream Control Transmission Protocol
fc 133 FC # Fibre Channel
rsvp-e2e-ignore 134 RSVP-E2E-IGNORE
135 # Mobility Header
udplite 136 UDPLite
mpls-in-ip 137 MPLS-in-IP
manet 138 manet # MANET Protocols
hip 139 HIP # Host Identity Protocol
140-252 Unassigned [IANA]
253 Use for experimentation and testing [RFC3692]
254 Use for experimentation and testing [RFC3692]
255 Reserved [IANA]