

P2P ENGELLEMELİK İÇİN QoS İLE CİSCO NBAR KULLANILMASI

Gökhan AKIN,
İstanbul Teknik Üniversitesi
Bilgi İşlem Daire Başkanlığı
akingok@itu.edu.tr

1.GİRİŞ

İstanbul Teknik Üniversitesi'nde bir süredir P2P trafiğini önlemek için Cisco yönlendirici ve üçüncü katman anahtarlama cihazlarında Quality of Service(QoS) ile Network-Based Application Recognition (NBAR) uygulaması denenmektedir.

QoS(servis kalitesi) gecikme ve bant genişliği bakımından hassas olan uygulamalara gereken şartları sağlamak için uygulanan çözümlerdir. Servis Kalitesini sağlamak için en yaygın kullanılan metot IP paket başlığında bulunan ToS(Type of Service) kısmına öncelik vermek amacı ile numara verilmesidir. Verilecek bu numara ile, yönlendirici interface'inde pakete öncelik verilebileceği gibi, paket çöpe de atılabilir. P2P uygulamaları da bu teknik ile trafik dışı bırakılabilir.

Uygulamalara öncelik vermek amaçlı yapılan QoS temel olarak TCP veya UDP port numaralarını göz önüne alır. Temel bazı uygulamalar sabit bir port numarası ile haberleştiği için bir gereken servis kalitesi sorunsuzca sağlanabilir. P2P yazılımları da başlangıçta sabit port numaraları ile haberleşmekte idiler. Ancak ağ yöneticileri bu trafikleri port bazlı kesebildiklerinden, günümüzde sabit port numarası kullanan P2P yazılımı kalmamış durumdadır. Günümüz P2P uygulamaları dinamik olarak port numarası alabildikleri gibi, kullanıcı elle başka uygulamanın (Örneğin 80 port HTTP gibi) bir uygulamanın numarasını atayarak haberleşmede yapabilmektedirler.

Bu sebepten port bazlı uygulama tespiti yerine imza tabanlı uygulama tespiti zorunlu hale gelmiştir. İmza tabanlı uygulama tespiti ağdan geçen bütün trafiğin veri (payload) kısmının kontrol edilip belirli bir örüntüye (pattern'e) uyup uymadığının kontrolü şeklinde yapılır. Bu amaçla Cisco yönlendirici cihazlarına IOS 12.0(5)XE2 versiyonundan sonra NBAR isimli uygulama eklenmiştir. NBAR paketlerin veri kısmını da inceleyerek uygulamanın ne olduğunu belirleyebilmektedir.

İmza tabanlı uygulama tespiti trafiğin başka bir porta yönlendirilip harici bir saldırı tespit cihazı ile yapılabileceği gibi bütün trafiğin içinden geçtiği cihazlarda (firewall veya yönlendiricilerde) inline olarak da yapılabilir. İlk çözümde TCP bazlı çalışan uygulamanın tespit edilmesinden sonra TCP END paketi yollanarak trafik durdurulabilir. Ancak UDP bazlı çalışan uygulamalar kesilememektedir. İkinci çözümde ise paketler direk inline cihaz tarafından çöpe atılabilir. Ancak buda paketlerde gecikme oluşabilmektedir. Bunların yanı sıra iki sistemde de bir hayli çok işlemci gücü gerekmektedir.

NBAR Cisco'nun geliştirdiği CEF (Cisco Express Forwarding) teknolojisini kullanmaktadır. CEF yönlendiricilerin daha hızlı anahtarlama yapabilmesi için Cisco'nun geliştirdiği bir teknolojidir. [1] CEF ile yönlendirici akan trafik için özel tablolar oluşturur ve aynı trafik devam ettiği sürece donanım olarak anahtarlama devam eder. CEF sayesinde NBAR trafikte pek bir gecikmeye sebep olmaz ve ayrıca yönlendiriciye de az bir işlemci yükü ekler.

2. NBAR KULLANILAMADIĞI DURUMLAR [2]

Aşağıda belirtilmiş durumlarda NBAR kullanılamaz.

1. IP dışındaki paketlerde.
2. MPLS etiketli paketlerde.
3. Fragment'e edilmiş paketlerde.
4. Kriptolama uygulanmış tünel interface'lerinde.
5. Multicast trafiklerde.
6. Etherchannel interface'lerinde.

3. NBAR KULLANIMI İÇİN GEREKEN ÖN ŞARTLAR

Öncelikle Cisco cihazınızın NBAR desteğine sahip olması gerekmekte ve cihazınıza NBAR desteğinin geldiği işletim sistemi (IOS) sürümünün yüklenmesi gerekmektedir. Ekte destekleyen cihazların listesini bulabilirsiniz. Ayrıca yönlendiricide CEF mutlaka açılmalıdır.

```
Router(config)# ip cef
```

Eğer Cisco 7500 yönlendiriciniz varsa Distributed CEF'i açmanız gerekmektedir.

```
ITU_7500(config)# ip cef distributed
```

4. NBAR İLE TANIMLANABİLEN P2P UYGULAMALARI [3]

NBAR'in şu andaki son IOS ile tanımlaya bildiği P2P uygulamaları tablodakilerdir. P2P'lerinin paket yapıları zamanla değişebildiği gibi yeni P2P uygulamalarda çıkmaktadır. Cisco her yeni uygulama için IOS upgrade yapılmasına gerek kalmaması için P2P imzalarını yönlendiricinin flash hafızasına sonrada yüklenebilecek modüler bir hale getirmiştir. Bu yapıya "Packet Description Language Modules" yani PDLM denilmektedir. NBAR ile tanımlanabilen diğer bütün uygulamaların listesi ekte bulunmaktadır.

Peer-to-Peer Protokolü	Tipi	Son PDLM Versiyonu
BitTorrent	TCP	3
Gnutella	TCP	6
Kazaa2	TCP/ UDP	6
eDonkey	TCP	3
Fasttrack	TCP	2
Napster	TCP	2
Direct Connect	TCP/ UDP	1
WinMX	TCP	2

5. NBAR KONFIGÜRASYONU

1. Üzerinde işlem yapılacak Trafiğin Tarifi

```
Router(config)# class-map match-any <Tanımlamanın İsmi>  
Router (config-cmap)#match protocol <Protokol İsmi>  
Router (config-cmap)#match protocol <Protokol İsmi>  
.....
```

2. Tarif edilmiş trafiğe yapılacak işlemin tanımı

Eğer trafik direk çöpe atılacak ise :

```
Router(config)#policy-map <İşlemin Grubunun Adı>  
Router(config-pmap)#class <Tanımlama İsmi>  
Router(config-pmap-c)# Drop
```

Eğer trafik sadece işaretlenecek ise :

```
Router(config)#policy-map <İşlemin Grubunun Adı>  
Router(config-pmap)#class <Tanımlama İsmi>  
Router(config-pmap-c)# set precedence <paketlere verilecek no (0 ile 7 arasında)>
```

3. Trafiğin Çöpe atılacağı zaman aralığının belirlenmesi

```
Router(config)#time-range <zaman_aralığı_adi>  
Router(config-time-range)# periodic weekdays 9:00 to 18:00
```

4. Trafiğin Belirlenen zaman aralığında Çöpe atılması için gereken tanımlama

```
Router(config)# access-list 100 deny ip any any precedence 2 time-range zaman_aralığı_adi
```

5. Yasaklamanın Interface'e uygulanması

```
Router(config)# interface <interface adi ve numarası>  
Router(config-if)# ip access-group 100 in
```

6. YENİ PDLM'LERİN YÖNLENDİRİCİYE YÜKLENMESİ

Son çıkan PDLM'ler "<http://www.cisco.com/cgi-bin/tablebuild.pl/pdlm>" adresinden temin edilebilir. Temin edilen PDLM'ler önce yönlendiricinin flash hafızasına kopyalanmalıdır. Daha sonra yönlendiriciye yeni PDLM'in adresi belirtilmelidir.

```
Router(config)#ip nbar pdlm flash:/<pdlm'in ismi>
```

Yüklenmiş olan PDLM'leri listelemek için aşağıdaki komut kullanılabilir.

```
Router#sh ip nbar pdlm
```

Yüklü olan PDLM'lerin versyonlarını listelemek için kullanılan komut aşağıdaki gibidir.

```
Router#sh ip nbar version
```

7. KİŞİYE ÖZEL PDLM TANIMLANMASI

Var olan PDLM'lerin yeterli olmaması durumunda yönlendiriciye o anki ihtiyaca göre özel PDLM tanımlanabilir. Bir yönlendiriciye maksimum 10 adet tanımlama yapılabilir. Ayrıca elle tanımlanan imzalarda paketin veri kısmının maksimum ilk 255 byte'lik kısmı incelenebilir.

Örnek PDLM Tanımlamaları:

```
Router(config)#ip nbar custom yeni_P2P 5 ascii ASIM source tcp range 8000 9000
```

Yukarıda "yeni_P2P" ismi ile tanımlanan PDLM, paketin veri kısmını ilk 5. byte'inde sonra "ASIM" ascii dizini bulunması durumunda ve paketin kaynağının tcp 8000 ile 9000 portları arasında olması durumunu tarif etmiştir.

8. NBAR İLE SADECE TRAFİK İSTATİSTİĞİNİN ÇIKARTILMASI

Trafik istatistiği yönlendirici üzerinde tutulabileceği gibi snmp ile yönlendiriciden bu bilgi çekilip MRTG gibi monitör programları ile loglanabilir. Ekte NBAR'ın SNMP MIB listesi bulunmaktadır.[4]

Yönlendirici üzerinde istatistik tutmak için interface konfigürasyon modunda aşağıdaki komut uygulanır.

```
Router(config-if)#ip nbar protocol-discovery
```

İstatistiğin incelemesi için

```
Router#sh ip nbar protocol-discovery
```

9. SONUÇ

İTÜ'de NBAR ile yapılan denemelerde hepsinde olmasa da bazı P2P uygulamalarında yüksek oranda tespit yüzdeleri gözlemlenmiştir. Zaman bazlı yazılabilen erişim kural listeleri ile de mesai saatleri içerisinde P2P trafiğinin yönlendiriciye fazla yük getirmeden kesilebileceği tespit edilmiştir. Ayrıca NBAR'ın "protokol-discovery" özelliği sayesinde ağ kullanımındaki trafik oranlarında gerçekçi olarak saptanabilmiştir.

EKLER:

EK1

Örnek Konfigurasyon:

```
ip nbar pdlm flash:/bittorrent.pdlm  
ip nbar pdlm flash:/directconnect.pdlm
```

....

```
class-map match-any peer-to-peer  
  match protocol directconnect  
  match protocol bittorrent  
  match protocol edonkey  
  match protocol gnutella  
  match protocol kazaa2  
  match protocol napster
```

....

```
policy-map peer-to-peer  
  class peer-to-peer  
    set precedence 2
```

....

```
access-list 100 deny ip any any precedence 2  
access-list 100 permit ip any any
```

....

```
interface FastEthernet0/0  
  service-policy input peer-to-peer
```

....

```
interface FastEthernet0/1  
  ip access-group 100 in
```

EK2 [2]

NBAR Destekleyen Cisco Yönlendiriciler:

- Cisco 800 Series Routers
- Cisco 1700 Series Modular Access Routers
- Cisco 1800 Series Integrated Services Routers
- Cisco 2600XM Series Router
- Cisco 2800 Series Integrated Services Routers
- Cisco 3700 Series Multiservice Access Routers
- Cisco 3800 Series Integrated Services Routers
- Cisco 7100 Series VPN Routers
- Cisco 7200 Series Routers
- Cisco 7300 Series Routers
- Cisco 7500 Series Routers
- Cisco Catalyst 6500

EK3 [2]

NBAR'ın Desteklediği Protokoller					
Protokol	Katagori	Tip	Well-Known Port Numaralari	Komut sentaksı	IOS Versiyonu
Citrix ICA	Enterprise Uygulama	TCP/UDP	Stateful Protocol	citrix citrix app	12.1(2)E 12.1(5)T
PCAnywhere	Enterprise Uygulama	TCP	5631, 65301	pcanywhere	12.0(5)XE2 12.1(1)E 12.1(5)T
PCAnywhere	Enterprise Application	UDP	22, 5632	pcanywhere	12.0(5)XE2 12.1(1)E 12.1(5)T
Novadigm	Enterprise Application	TCP/UDP	3460- 3465	novadigm	12.1(2)E 12.1(5)T
SAP	Enterprise Application	TCP	3300-3315 (sap-pgm. pdlm) 3200-3215 (sap-app. pdlm) 3600-3615 (sap-msg. pdlm)	sap	12.3 12.3 T 12.2 T 12.1 E
BGP	Routing Protocol	TCP/UDP	179	bgp	12.0(5)XE2 12.1(1)E 12.1(5)T
EGP	Routing Protocol	IP	8	egp	12.0(5)XE2 12.1(1)E 12.1(5)T
EIGRP	Routing Protocol	IP	88	eigrp	12.0(5)XE2 12.1(1)E 12.1(5)T
OSPF	Routing Protocol	TCP	Stateful Protocol	ospf	12.3(8)T
RIP	Routing Protocol	UDP	520	rip	12.0(5)XE2 12.1(1)E 12.1(5)T
SQL*NET	Database	TCP/UDP	Stateful Protocol	sqlnet	12.0(5)XE2 12.1(1)E 12.1(5)T

MS-SQLServer	Database	TCP	1433	sqlserver	12.0(5)XE2 12.1(1)E 12.1(5)T
GRE	Security and Tunneling	IP	47	gre	12.0(5)XE2 12.1(1)E 12.1(5)T
IPINIP	Security and Tunneling	IP	4	ipinip	12.0(5)XE2 12.1(1)E 12.1(5)T
IPSec	Security and Tunneling	IP	50, 51	ipsec	12.0(5)XE2 12.1(1)E 12.1(5)T
L2TP	Security and Tunneling	UDP	1701	l2tp	12.0(5)XE2 12.1(1)E 12.1(5)T
MS-PPTP	Security and Tunneling	TCP	1723	pptp	12.0(5)XE2 12.1(1)E 12.1(5)T
SFTP	Security and Tunneling	TCP	990	secure-ftp	12.0(5)XE2 12.1(1)E 12.1(5)T
SHTTP	Security and Tunneling	TCP	443	secure-http	12.0(5)XE2 12.1(1)E 12.1(5)T
SIMAP	Security and Tunneling	TCP/ UDP	585, 993	secure-imap	12.0(5)XE2 12.1(1)E 12.1(5)T
SIRC	Security and Tunneling	TCP/ UDP	994	secure-irc	12.0(5)XE2 12.1(1)E 12.1(5)T
SLDAP	Security and Tunneling	TCP/ UDP	636	secure-ldap	12.0(5)XE2 12.1(1)E 12.1(5)T
SNNTTP	Security and Tunneling	TCP/ UDP	563	secure-nntp	12.0(5)XE2 12.1(1)E 12.1(5)T
SPOP3	Security and Tunneling	TCP/ UDP	995	secure-pop3	12.0(5)XE2 12.1(1)E 12.1(5)T
STELNET	Security and Tunneling	TCP	992	secure-telnet	12.0(5)XE2 12.1(1)E 12.1(5)T
SOCKS	Security and Tunneling	TCP	1080	socks	12.0(5)XE2 12.1(1)E

					12.1(5)T
SSH	Security and Tunneling	TCP	22	ssh	12.0(5)XE2 12.1(1)E 12.1(5)T
ICMP	Network Management	IP	1	icmp	12.0(5)XE2 12.1(1)E 12.1(5)T
SNMP	Network Management	TCP/ UDP	161, 162	snmp	12.0(5)XE2 12.1(1)E 12.1(5)T
Syslog	Network Management	UDP	514	syslog	12.0(5)XE2 12.1(1)E 12.1(5)T
IMAP	Network Mail Services	TCP/ UDP	143, 220	imap	12.0(5)XE2 12.1(1)E 12.1(5)T
POP3	Network Mail Services	TCP/ UDP	110	pop3	12.0(5)XE2 12.1(1)E 12.1(5)T
Exchange	Network Mail Services	TCP	MS-RPC for Exchange	TCP	12.0(5)XE2 12.1(1)E 12.1(5)T
Notes	Network Mail Services	TCP/ UDP	1352	notes	12.0(5)XE2 12.1(1)E 12.1(5)T
SMTP	Network Mail Services	TCP	25	smtp	12.0(5)XE2 12.1(1)E 12.1(5)T
DHCP/ BOOTP	Directory	UDP	67, 68	dhcp	12.0(5)XE2 12.1(1)E 12.1(5)T
Finger	Directory	TCP	79	finger	12.0(5)XE2 12.1(1)E 12.1(5)T
DNS	Directory	TCP/ UDP	53	dns	12.0(5)XE2 12.1(1)E 12.1(5)T
Kerberos	Directory	TCP/ UDP	88, 749	kerberos	12.0(5)XE2 12.1(1)E 12.1(5)T
LDAP	Directory	TCP/ UDP	389	ldap	12.0(5)XE2 12.1(1)E 12.1(5)T

CU-SeeMe	Streaming Media	TCP/UDP	7648, 7649	cuseeme	12.0(5)XE2 12.1(1)E 12.1(5)T
CU-SeeMe	Streaming Media	UDP	24032	cuseeme	12.0(5)XE2 12.1(1)E 12.1(5)T
Netshow	Streaming Media	TCP/UDP	Stateful Protocol	netshow	12.0(5)XE2 12.1(1)E 12.1(5)T
RealAudio	Streaming Media	TCP/UDP	Stateful Protocol	realaudio	12.0(5)XE2 12.1(1)E 12.1(5)T
StreamWorks	Streaming Media	UDP	Stateful Protocol	streamwork	12.0(5)XE2 12.1(1)E 12.1(5)T
VDOLive	Streaming Media	TCP/UDP	Stateful Protocol	vdolive	12.0(5)XE2 12.1(1)E 12.1(5)T
RTSP	Streaming Media/ Multimedia	TCP/UDP	Stateful Protocol	rtsp	12.3(11)T
MGCP	Streaming Media/ Multimedia	TCP/UDP	2427, 2428, 2727	mgcp	12.3(7)T
FTP	Internet	TCP	Stateful Protocol	ftp	12.0(5)XE2 12.1(1)E 12.1(5)T
Gopher	Internet	TCP/UDP	70	gopher	12.0(5)XE2 12.1(1)E 12.1(5)T
HTTP	Internet	TCP	80	http	12.0(5)XE2 12.1(1)E 12.1(5)T
IRC	Internet	TCP/UDP	194	irc	12.0(5)XE2 12.1(1)E 12.1(5)T
Telnet	Internet	TCP	23	telnet	12.0(5)XE2 12.1(1)E 12.1(5)T
TFTP	Internet	UDP	Stateful Protocol	tftp	12.0(5)XE2 12.1(1)E 12.1(5)T
NNTP	Internet	TCP/UDP	119	nntp	12.0(5)XE2 12.1(1)E

					12.1(5)T
RSVP	Signaling	UDP	1698, 1699	rsvp	12.0(5)XE2 12.1(1)E 12.1(5)T
NFS	RPC	TCP/ UDP	2049	nfs	12.0(5)XE2 12.1(1)E 12.1(5)T
Sunrpc	RPC	TCP/ UDP	Stateful Protocol	sunrpc	12.0(5)XE2 12.1(1)E 12.1(5)T
NetBIOS	nonIP and LAN/ Legacy	TCP/ UDP	137, 138, 139	netbios	12.0(5)XE2 12.1(1)E 12.1(5)T
NTP	Misc.	TCP/ UDP	123	ntp	12.0(5)XE2 12.1(1)E 12.1(5)T
Printer	Misc.	TCP/ UDP	515	printer	12.1(2)E 12.1(5)T
X Windows	Misc.	TCP	6000-6003	xwindows	12.0(5)XE2 12.1(1)E 12.1(5)T
r-commands	Misc.	TCP	Stateful Protocol	rcmd	12.0(5)XE2 12.1(1)E 12.1(5)T
H.323	Voice	TCP	Stateful Protocol	h323	12.3.(7)T
RTCP	Voice	TCP/ UDP	Stateful Protocol	rtcp	12.1E 12.2T 12.3 12.3T 12.3(7)T
RTP	Voice	TCP/ UDP	Stateful Protocol	rtp	12.2(8)T
SIP	Voice	TCP/UPD	5060	sip	12.3(7)T
SCCP/ Skinny	Voice	TCP	2000, 2001, 2002	skinny	12.3(7)T
Skype	Voice	TCP/ UPD	Stateful Protocol	skype	12.4(4)T
BitTorrent	Peer-to-Peer file sharing applications	TCP	Stateful Protocol, or 6881-6889	bittorrent	12.4(2)T
Direct Connect	Peer-to-Peer file sharing	TCP/ UDP	411	directconnect	12.4(4)T

	applications				
eDonkey/ eMule	Peer-to-Peer file sharing applications	TCP	4662	edonkey	12.3(11)T
FastTrack	Peer-to-Peer file sharing applications	N/A	Stateful Protocol	fasttrack	12.1(12c)E
Gnutella	Peer-to-Peer file sharing applications	TCP	Stateful Protocol	gnutella	12.1(12c)E
KaZaA	Peer-to-Peer file sharing applications	TCP/ UPD	Stateful Protocol	kazaa2	12.2(8)T
WinMX	Peer-to-Peer file sharing applications	TCP	6699	winmx	12.3(7)T

EK4 [4]

NBAR'in SNMP MIB Listesi

iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.1 = STRING: "ftp"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.2 = STRING: "http"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.3 = STRING: "egp"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.4 = STRING: "gre"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.5 = STRING: "icmp"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.6 = STRING: "eigrp"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.7 = STRING: "ipinip"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.8 = STRING: "ipsec"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.9 = STRING: "bgp"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.10 = STRING: "cuseeme"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.11 = STRING: "dhcp"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.12 = STRING: "dns"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.13 = STRING: "finger"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.14 = STRING: "gopher"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.15 = STRING: "secure-http"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.16 = STRING: "imap"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.17 = STRING: "secure-imap"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.18 = STRING: "irc"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.19 = STRING: "secure-irc"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.20 = STRING: "kerberos"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.21 = STRING: "l2tp"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.22 = STRING: "ldap"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.23 = STRING: "secure-ldap"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.24 = STRING: "sqlserver"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.25 = STRING: "netbios"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.26 = STRING: "nfs"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.27 = STRING: "nntp"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.28 = STRING: "secure-nntp"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.29 = STRING: "notes"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.30 = STRING: "ntp"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.31 = STRING: "pcanywhere"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.32 = STRING: "pop3"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.33 = STRING: "secure-pop3"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.34 = STRING: "pptp"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.35 = STRING: "rip"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.36 = STRING: "rsvp"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.37 = STRING: "smtp"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.38 = STRING: "snmp"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.39 = STRING: "socks"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.40 = STRING: "ssh"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.41 = STRING: "syslog"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.42 = STRING: "telnet"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.43 = STRING: "secure-telnet"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.44 = STRING: "secure-ftp"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.45 = STRING: "xwindows"

iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.46 = STRING: "printer"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.47 = STRING: "novadigm"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.48 = STRING: "tftp"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.49 = STRING: "exchange"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.50 = STRING: "vdolive"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.51 = STRING: "sqlnet"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.52 = STRING: "rcmd"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.53 = STRING: "netshow"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.54 = STRING: "sunrpc"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.55 = STRING: "streamwork"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.56 = STRING: "citrix"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.57 = STRING: "napster"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.58 = STRING: "fasttrack"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.59 = STRING: "gnutella"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.60 = STRING: "kazaa2"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.61 = STRING: "custom-01"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.62 = STRING: "custom-02"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.63 = STRING: "custom-03"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.64 = STRING: "custom-04"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.65 = STRING: "custom-05"
iso.3.6.1.4.1.9.9.244.1.2.1.1.2.1.66 = STRING: "custom-06"

KAYNAKLAR

[1] How to Choose the Best Router Switching Path for Your Network,
http://www.cisco.com/en/US/tech/tk827/tk831/technologies_white_paper09186a00800a62d9.shtml#express

[2] Network-Based Application Recognition and Distributed Network-Based Application Recognition, <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121e/121e1/dtnbarad.htm>

[3] Network-Based Application Recognition, http://www.cisco.com/en/US/products/ps6616/products_case_study09186a00800ad0ca.shtml

[4] Graphing Cisco Systems (NBAR) Network-based application recognition with MRTG,
http://vermeer.org/display_doc.php?doc_id=6