IBM Security QRadar
Version 7.1.0 (MR2)

Application Configuration Guide

Note: Before using this information and the product that it supports, read the information in “Notices and Trademarks” on page 53.

CONTENTS

ABOUT THIS GUIDE

The *IBM Security QRadar Application Configuration Guide* provides you with information on how to configure application mappings. Defining custom applications enables QRadar to classify applications used in a flow and is useful when you investigate various types of security threats using the Offenses, Log Activity, or Network Activity tabs.

Intended Audience

The guide is intended for the system administrator responsible for configuring application mappings in your QRadar deployment. This guide assumes that you have QRadar administrative access and a knowledge of your corporate network and networking technologies.

Conventions

The following conventions are used throughout this guide:

▶ Indicates that the procedure contains a single instruction.

Note: Indicates that the information provided is supplemental to the associated feature or instruction.

CAUTION: *Indicates that the information is critical. A caution alerts you to potential loss of data or potential damage to an application, system, device, or network.*

WARNING: *Indicates that the information is critical. A warning alerts you to potential dangers, threats, or potential personal injury. Read any and all warnings carefully before proceeding.*

Technical Documentation	For information on how to access more technical documentation, technical notes, and release notes, see the ***Accessing IBM Security QRadar Documentation Technical Note***. (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21614644)
Contacting Customer Support	For information on contacting customer support, see the ***Support and Download Technical Note***. (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861)
Statement of good security practices	IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

1 APPLICATION MAPPING

QRadar includes default application IDs, however, you can edit the application mapping file to ensure traffic is appropriately classified in the QRadar user interface.

About QRadar applications

When QRadar detects a flow, it assigns an application ID to the flow, based on the content of the flow, the protocol used for the flow, and the ports.

QRadar includes default application IDs, however, you can edit the application mapping file to ensure traffic is appropriately classified in the QRadar user interface. The mappings in the mapping file override the default application IDs. For more information about default application IDs, see **Default applications**.

Overview of application mapping tasks

When you create a new or customized application mapping, you must edit configuration files using SSH.

Perform the following tasks in sequence:

1. **Define applications** - The application configuration file contains default applications. To define new applications, you must add new applications IDs to the application configuration file. For more information, see **Defining new applications**.
2. **Map traffic to the applications** - You must also map traffic to the applications you defined. You can map traffic to the applications using one, or both, of the following methods:
   - **Define application mappings** - Update the application mapping file, which maps applications to application IDs based on IP address and port number. For more information, see **Defining application mappings**.
   - **Define application signatures** - Define application signatures to apply to flows that the default application mapping could not automatically detect. This method involves creating rules, based on IP address, port, and content, to assign application IDs to flows. For more information, see **Defining application signatures**. To define port-only application signatures, you must configure port mappings using the application mapping file, not the application signatures file.

Defining new applications

Edit the application configuration file to define new applications.

About this task

When inserting new applications, note the following considerations:

- When you add new application ID numbers, you must create a new and unique application ID number. The application ID number must not already exist in the apps.conf file. We recommend that you apply numbers that range between 15,000 to 20,000 for custom applications. Contact Customer Support for further information.
- The format of the entry uses the following syntax:

  <appname><newID>

  Where:

  - **<appname>** is the name of the application. The application name is used in the **Network Activity** and **Offenses** tabs. You can specify an application name with up to five application levels; however, QRadar only uses three levels of the application name. Each level of the application name must be separated using the number sign (#).
  - **<appid>** is the unique ID for each application that you want to define.

  The following example defines the Authentication.Radius-1646 application with an application ID of 51343:

  Authentication#Radius-1646####51343
- Five application levels are represented in the application ID. Application levels are separated by number sign (#). If an application ID contains less than five levels, you must include the number signs for all five levels.
- You must insert the new application ID in alphabetical order in the apps.conf file.

  For example: To add **Authentication#Radius-1646####51343** as an application ID, insert the applciation ID as follows:

```
Authentication#Radius-1645####51342
Authentication#Radius-1646####51343 <- inserted application
Authentication#Radius-1812####51344
Authentication#Radius-1813####51345
```

Procedure

Step 1 Using SSH, log in to QRadar as the root user.

Username: **root**

Password: **<password>**

Step 2 Open the following file:

/store/configservices/staging/globalconfig/apps.conf

Step 3 Insert new applications, as necessary.

Step 4 Save and exit the file.

Step 5 Log in to the QRadar user interface.

Step 6 Click the **Admin** tab.

Step 7 On the toolbar, click **Deploy Changes**.

What to do next

Choose one of the following options:

- To define application mappings, see **Defining application mappings**.
- To define application signatures, see **Defining application signatures**.

Defining application mappings

Using the application mapping file, you can create user-defined application mappings based on the IP address and port number.

Before you begin

Before you begin, you must have added new application IDs. See **Defining new applications**.

About this task

When updating the file, note the following:

- Each line in the file indicates a mapped application. You can specify multiple mappings (each on a separate line) for the same application.
- You can specify a wildcard character * for any field. Use the wildcard character alone, and not as part of a comma-separated list. The wildcard character indicates that the field applies to all flows.
- A flow can be associated with multiple mappings; therefore, a flow is mapped to an application ID based on the mapping order in the file. The first mapping that applies in the file is assigned to the flow.
- When you add new application ID numbers, you must create a new and unique application ID number. The application ID number must not already exist in the apps.conf file. We recommend that you apply numbers that range between 15,000 to 20,000 for custom applications. Contact Customer Support for further information.
- The format of the entry must resemble the following:

  ```
  <New ID> <Old ID> <Source IP Address>:<Source Port> <Dest IP Address>:<Dest Port> <Name>
  ```

  Where:

  - **<New ID>** specifies the application ID you want to assign to the flow. A value of 1 indicates an unknown application. If the ID you want to assign does not exist, you must create the ID in the apps.conf file. For more information, see **Defining new applications**.

- **<Old ID>** specifies the default application ID of the flow, as assigned by QRadar. A value of * indicates a wildcard character. If multiple application IDs are assigned, the application IDs are separated by commas.

To determine the default application IDs, go to the Network Activity tab in the QRadar user interface. Move your mouse pointer over the application field for a flow associated with the application you want to update to display the application ID. For more information about default values, see **Default applications**.

- **<Source IP Address>** specifies the source IP address of the flow. This field can contain either a comma-separated list of addresses or (Classless Inter-Domain Routing) CIDR values. A value of * indicates a wildcard character, which means that this field applies to all flows.
- **<Source Port>** specifies the associated port. This field can contain a comma-separated list of values or ranges specified in the format: <lower port number>-<upper port number>. A value of * indicates a wildcard character, which means that this field applies to all flows.
- **<Dest IP Address>** specifies the destination IP address of the flow. This field can contain either a comma-separated list of addresses or CIDR values. A value of * indicates a wildcard character, which means that this field applies to all flows.
- **<Dest Port>** specifies the associated destination port. This field can contain a comma-separated list of values or ranges specified in the format: <lower port number>-<upper port number>. A value of * indicates a wildcard character, which means that this field applies to all flows.
- **<Name>** specifies a name you want to assign to this mapping. This field is optional.

The following example maps all flows that match the IP addresses and ports for which the QRadar QFlow Collector has assigned to the Old ID of 1010 and assign the new ID of 15000:

```
15000 1010 10.100.100/24,10.100.50.10:* 172.14.33.33:80,443
```

Example 1 of mapping file

```
15000 1010 10.100.100/24,10.100.50.10:* 172.14.33.33:80,443
AllowedWebTypeA
15000 1010 10.100.30/24:* 172.14.33.20:80 AllowedWebTypeA
15100 * *:33333
64.35.20/24,64.33/16,64.77.34.12:33333,33350-33400 GameX
15100 1,34803,34809 *:33333 *:33333,33350-33400 GameX
```

Example 2 of mapping file

```
21200   1,34803,34809   *:*     *:123   ntp
34731   1,34803,34809   *:*     *:1241  Nessus
2001    1,34803,34809   *:*     *:1214  Kazaa
```

Procedure

Step 1 Using SSH, log in to QRadar as the root user.

Username: **`root`**

Password: **`<password>`**

Step 2 Choose one of the following options:

- Open the following file:

  `/store/configservices/staging/globalconfig/user_application_mapping.conf`

- If the user_application_mapping.conf does not exist in your system, create the file and place the empty file in the following directory: /store/configservices/staging/globalconfig/

Step 3 Update the file, as necessary.

Step 4 Save and exit the file.

Step 5 If necessary, edit your application configuration file.

Step 6 Log in to the QRadar user interface.

Step 7 Click the **Admin** tab.

Step 8 Click **Deploy Changes**.

Defining application signatures

Using the application signatures file, you can create IP address and content-based rules to assign application IDs to flows that QRadar does not automatically detect.

About this task

The application signatures file is a definition file distributed to all QRadar QFlow Collectors by the primary Console. The file includes source and destination ports, and ranges.

Characteristics of the application signatures file include:

- Hex content is delimited with the pipe character "**|**". For example: **`<dstcontent offset="0" depth="4">|45 54|</dstcontent>`** or, **`<dstcontent offset="0" depth="4">GET</dstcontent>`**
- A flow can be associated with multiple signatures; therefore, a flow is mapped to an application ID based on the signature order in the file. The first signature that applies in the file is assigned to the flow.
- When editing the signatures.xml file, the data inserted between the XML tags is case-sensitive. For example, when specifying TCP within the XML tags, you must enter the value using all capital letters.
- We recommend that you include the user_defined parameter in your new or updated signature. This parameter ensures all modification are maintained after an automatic update.

For a list of default application identification numbers, see **Default applications**.

When you edit the Applications Signature file, use the following parameters:

Table 1-1 Application Signatures default parameters

Parameter	Description
appid	Type a unique ID for each application that you want to define. We recommend that you apply numbers that range between 15,000 to 20,000 for custom applications. Contact Customer Support for further information.
appname	Type the name of the application. The application name is used in the Network Activity and Offenses tabs.
groupname	Type the group name for the application. ***Note:*** *This parameter is currently only used with the exception of the automatic generation script.*
description	Type the long description of the application and any required notes for the particular signature.
revision	Type a revision for version control.
protocol	Type the protocol. If the same signature is required for more than one protocol, define the second signature.
srcip	Type the specific source IP address for the signature to execute. Use multiple application identifications if more than one source IP address is required.
srcport	Type the specific source port for the signature to execute. Use multiple application identifications if more than one source port is required.
dstip	Type the specific destination IP address for the signature to execute. Use multiple application identifications if more destination IP addresses are required.
dstport	Type the specific destination port for the signature to execute. Use multiple application identifications if more than one destination port is required.
commondstport	Type the destination port most commonly associated with the application.
commonsrcport	Type the source port most commonly associated with the application.
scrcontent <offset> <depth>	Type the following options: **<offset>** is the offset in the payload that you want to begin searching for the source content. If no value is specified, the default is 0. **<depth>** is the offset in the payload you want to stop the search. For example, if you configure the following: `scrcontent 5 10` The payload would be searched between 5 and 15 bytes.

Table 1-1 Application Signatures default parameters (continued)

Parameter	Description
dstcontent <offset> <depth>	Type the following options: **<offset>** is the offset in the payload that you want to begin searching for the destination content. If no value is specified, the default is 0. **<depth>** is the offset in the payload you want to stop the search. For example, if you configure the following: **scrcontent 5 10** The payload would be searched between 5 and 15 bytes.
weight	Type the weight you want to assign this application.
user_defined	Specify to ensure that a new or updated signature is maintained after an automatic update. ***Note:*** *For more information regarding automatic updates, see the IBM Security QRadar SIEM Administration Guide.*

Example of a Signatures.xml file

```
<signatures>
<signature>
   <appid>1009</appid>
   <appname>IMAP</appname>
   <groupname>Mail</groupname>
   <colour>#ff0000</colour>
   <description>IMAP traffic</description>
   <revision>1</revision>
   <protocol>TCP</protocol>
   <srcip>any</srcip>
   <srcport>any</srcport>
   <dstip>any</dstip>
   <dstport>any</dstport>
   <commondstport>143</commondstport>
   <srccontent offset="0" depth="128"
   ignorecase="true">LOGIN</srccontent>
   <dstcontent offset="0" depth="5">* OK</dstcontent>
   <weight>30</weight>
</signature>
</signatures>
```

Procedure

Step 1 Using SSH, log in to QRadar as the root user.

Username: `root`

Password: `<password>`

Step 2 To change to the `globalconfig` directory, type the following command:

```
cd /store/configservices/staging/globalconfig
```

Step 3 Open the following file:

```
signatures.xml
```

Step 4 Make the necessary changes. See **Table 1-1**.

Step 5 Save and exit the file.

Step 6 If necessary, edit your applications configuration file. See **Defining new applications**.

Step 7 Log in to QRadar.

Step 8 Click the **Admin** tab.

Step 9 Click **Deploy Changes**.

2 DEFAULT APPLICATIONS

QRadar includes default application IDs, which you can view in the applications configuration file. The default application values apply to all source and destination flows; however, the destination port is specific to the application.

The following table provides the default Application values for QRadar:

Table 2-1 Default applications

Application group	Sub-components	Value	Description
Authentication	LDAP	1019	LDAP traffic
Authentication	MSGAuthentication	20998	MSG authentication traffic
Authentication	NTLMSSP	5700	NT LAN Manager Support Provider (NTLMSSP) traffic
Authentication	Radius	51342	Radius traffic
Authentication	Radius	51344	Radius traffic
Authentication	Radius	51345	Radius traffic
Authentication	tacacs	21028	Tacacs traffic
Authentication	TACACS-DatabaseService	21061	Tacacs Database Service traffic
Chat	CUSeeMe	60016	CUSeeMe traffic
Chat	iChat	3008	iChat traffic
Chat	ICQ	268435456	ICQ traffic
Chat	ICQ	3001	ICQ traffic
Chat	ICQ	3002	ICQ traffic
Chat	ICQControl	285212672	ICQ traffic
Chat	ICQTalk	301989888	ICQ traffic
Chat	IRC	5669	IRC traffic
Chat	IRC	5782	IRC traffic
Chat	IRC	5668	IRC traffic
Chat	IRC	3003	IRC traffic
Chat	Jabber	3004	Jabber protocol traffic
Chat	Jabber	3006	Jabber protocol traffic
Chat	Jabber	3005	Jabber protocol traffic

Table 2-1 Default applications (continued)

Application group	Sub-components	Value	Description
Chat	Lotus-IM	60162	Lotus IM traffic
Chat	MSN	3000	MSN traffic
Chat	MSN	5672	MSN traffic
Chat	MSN	5685	MSN traffic
Chat	MSN	5695	MSN traffic
Chat	MSN	5832	MSN traffic
Chat	MSN	5847	MSN traffic
Chat	MSN	318767104	MSN traffic
Chat	MSN	5831	MSN traffic
Chat	MSN > MSNFolderShare	321650688	MSN folder sharing traffic
Chat	MSN > MSNVideo	321781760	MSN video traffic
Chat	MSN> MSNFileTransfer	321650688	MSN file transfer traffic
Chat	Windows-POPUP	60170	Windows Messenger Service Pop-up
Chat	Yahoo	1033	Yahoo traffic
ClientServer	CitrixIMA	60115	Citrix IMA traffic
ClientServer	CVSpserver	60150	CVS traffic
ClientServer	CVSup	60129	CVS traffic
ClientServer	FIX	60057	FIX traffic
ClientServer	FoldingAtHome	60121	FoldingAtHome traffic
ClientServer	INFOC-RTMS	60102	RTMS information traffic
ClientServer	INT-1	60111	INT-1 server traffic
ClientServer	MATIP	60101	MATIP traffic
ClientServer	MeetingMaker	60108	Meeting maker traffic
ClientServer	NetIQ	60127	NetIQ traffic
ClientServer	PEPGate	60104	PEPGate traffic
ClientServer	Unisys-TCPA	60105	Unisys TCPA traffic
ContentDelivery	Ariel-419	60166	Ariel content delivery
ContentDelivery	Ariel-422	60167	Ariel content delivery
ContentDelivery	BackWeb	60024	BackWeb traffic
ContentDelivery	Chaincast	60156	Chaincast traffic
ContentDelivery	EntryPoint	60000	EntryPoint traffic
ContentDelivery	Kontiki	60148	Kontiki traffic
ContentDelivery	NewsStand	60146	New stand traffic
ContentDelivery	Webshots	60147	Webshots Desktop traffic

Table 2-1 Default applications (continued)

Application group	Sub-components	Value	Description
DataTransfer	AFS	60126	AFS file system traffic
DataTransfer	Apple-iTunes	60163	iTunes traffic
DataTransfer	BITS	60178	Background intelligent transfer service (Windows Updates)
DataTransfer	CU-Dev	60070	CU-dev traffic
DataTransfer	DLS	60002	DLS traffic
DataTransfer	FNAonTCP	60069	FNA traffic
DataTransfer	FTP	27720	File Transfer Protocol (FTP) traffic
DataTransfer	FTP	27719	File Transfer Protocol (FTP) traffic
DataTransfer	FTP	1002	File Transfer Protocol (FTP) traffic
DataTransfer	FTP	5787	File Transfer Protocol (FTP) traffic
DataTransfer	FTP	5788	File Transfer Protocol (FTP) traffic
DataTransfer	FTP	5789	File Transfer Protocol (FTP) traffic
DataTransfer	FTP	5820	File Transfer Protocol (FTP) traffic
DataTransfer	FTP	5833	File Transfer Protocol (FTP) traffic
DataTransfer	FTP	5821	File Transfer Protocol (FTP) traffic
DataTransfer	FTP	5845	File Transfer Protocol (FTP) traffic
DataTransfer	FTP	5844	File Transfer Protocol (FTP) traffic
DataTransfer	FTPControl	150994944	File Transfer Protocol (FTP) traffic
DataTransfer	FTPData	167772160	File Transfer Protocol (FTP) traffic
DataTransfer	lockd	60068	lockd traffic
DataTransfer	Microsoft-ds	60142	Microsoft® directory server traffic
DataTransfer	Misc-Transfer-Ports	21919	Misc common data traffic ports
DataTransfer	Misc-Transfer-Ports	22012	Misc common data traffic ports
DataTransfer	MSMQ	34806	MSMQ traffic
DataTransfer	NetBIOS-IP	60013	Windows/Netbios networking
DataTransfer	NFS	51349	Network File System (NFS) traffic

Table 2-1 Default applications (continued)

Application group	Sub-components	Value	Description
DataTransfer	NFS	1007	Network File System (NFS) traffic
DataTransfer	NNTPNews	51335	NNTP traffic
DataTransfer	NNTPNews	1013	NNTP traffic
DataTransfer	NortonGhost	60194	Norton Ghost traffic
DataTransfer	NW5-CMD	60078	Netware traffic
DataTransfer	NW5-NCP	60076	Netware traffic
DataTransfer	SHARESUDP	60106	UDP sharing traffic
DataTransfer	SunND	60173	Sun ND traffic
DataTransfer	TFTP	251658240	TFTP traffic
DataTransfer	TFTP	21930	TFTP traffic
DataTransfer	TFTP	1003	TFTP traffic
DataTransfer	UUCP	60012	UUCP traffic
DataTransfer	WindowsFileSharing	1014	Windows file sharing
DataTransfer	WindowsFileSharing	1021	Windows file sharing
DataTransfer	WindowsNetworkPorts	51340	NETBIOS. Windows networking
DataTransfer	WindowsNetworkPorts	51339	NETBIOS. Windows networking
DataTransfer	WindowsNetworkPorts	51338	NETBIOS. Windows networking
DataWarehousing	ARCserverBackup	34730	ARC server backup
DataWarehousing	BAAN	60082	BAAN traffic
DataWarehousing	dbase	35298	dbase traffic
DataWarehousing	FileMaker	60112	FileMaker traffic
DataWarehousing	Filenet	34800	Filenet traffic
DataWarehousing	GuptaSQLBase	34841	GuptaSQLBase traffic
DataWarehousing	JDENet	60099	JDENet traffic
DataWarehousing	Misc-DB	51249	Oracle list service
DataWarehousing	Misc-DB	39045	Oracle list service
DataWarehousing	MSSQLServer	10002	Database MS SQL Server
DataWarehousing	MySQL	37291	MySQL traffic
DataWarehousing	ORA	37302	ORA traffic
DataWarehousing	Oracle	37751	Oracle traffic
DataWarehousing	Oracle	37762	Oracle traffic
DataWarehousing	oracle	37289	Oracle traffic
DataWarehousing	Oracle	38292	Oracle traffic
DataWarehousing	Oracle	37290	Oracle traffic
DataWarehousing	Oracle	42069	Oracle traffic
DataWarehousing	Oracle	37914	Oracle traffic

Table 2-1 Default applications (continued)

Application group	Sub-components	Value	Description
DataWarehousing	Oracle	37871	Oracle traffic
DataWarehousing	Oracle	37870	Oracle traffic
DataWarehousing	Oracle	37512	Oracle traffic
DataWarehousing	Oracle	37401	Oracle traffic
DataWarehousing	OracleClient	60086	OracleClient traffic
DataWarehousing	OracleDB	37394	Oracle DB traffic
DataWarehousing	OracleTNS	134217728	Oracle TNS traffic
DataWarehousing	OracleTNS > MsForms	136511488	Oracle TNS traffic
DataWarehousing	OracleTNS > MsODBC	136314880	Oracle TNS traffic
DataWarehousing	OracleTNS > MsOLE	136380416	Oracle TNS traffic
DataWarehousing	OracleTNS > MsSQLPlus	136445952	Oracle TNS traffic
DataWarehousing	OracleTNS > PeopleSoft	136577024	Oracle TNS traffic
DataWarehousing	orasrv	37299	Orasrv traffic
DataWarehousing	PostgreSQL	37292	PostgreSQL traffic
DataWarehousing	Progress	60110	Progress traffic
DataWarehousing	SAP	40695	SAP R/3 application server
DataWarehousing	SAPGatewayServer	40456	SAPGateway Server traffic
DataWarehousing	SQL-NET	34923	SQL-NET traffic
DirectoryServices	CRS	60060	CRS traffic
DirectoryServices	Ident	60059	Ident traffic
DirectoryServices	LDAP	34801	LDAP traffic
DirectoryServices	LDAP	51341	LDAP traffic
DirectoryServices	mDNS	60183	mDNS traffic
DirectoryServices	RRP	60133	RRP traffic
DirectoryServices	SSDP	60158	SSDP traffic
DirectoryServices	WINS	60088	WINS traffic
FilePrint	IPP	60097	IPP traffic
FilePrint	MDQS	60195	MQDS traffic
FilePrint	Printer	60051	Printer traffic
FilePrint	tn3287	60062	tn3287 traffic
FilePrint	tn5250p	60064	tn5250p traffic
FileTransfer	DCOM	51336	DCOM traffic
FileTransfer	NETBIOS	51337	Windows/Netbios networking
FileTransfer	netcp	35159	NetCp traffic
FileTransfer	NIFTP	21879	National Instruments File Transfer Protocol traffic

Table 2-1 Default applications (continued)

Application group	Sub-components	Value	Description
FileTransfer	PrivateFileService	21910	Private File Service traffic
FileTransfer	xfer	21984	XFER traffic
Games	AsheronsCall	60122	AsheronsCall traffic
Games	BattleNet	60116	Battle.net traffic
Games	Doom	60039	Doom traffic
Games	Half-Life	60119	Half-life traffic
Games	Kali	60042	Kali traffic
Games	LucasArts	60157	LucasArts traffic
Games	MSN-Zone	60123	MSN-Zone traffic
Games	Mythic	60149	Mythic traffic
Games	Quake	60040	Quake traffic
Games	SonyOnline	60138	SonyOnline traffic
Games	Tribes	60124	Tribes traffic
Games	Unreal	60117	Unreal traffic
Games	YahooGames	60120	YahooGames traffic
Healthcare	DICOM	60143	DICOM traffic
Healthcare	HL7	60154	HL7 traffic
InnerSystem	Common-Ports	51334	Flow traffic o
InnerSystem	Flowgen	1023	QFlow Collector and flow traffic
InnerSystem	UpdateDaemon	1024	Update Daemon traffic
InternetProtocol	ActiveX	60056	ActiveX traffic
InternetProtocol	IPHeaderCompression	34843	IPHeaderCompression traffic
InternetProtocol	SOAP-HTTP	60179	SOAP-HTTP traffic
Legacy	AFP	60058	AFP traffic
Legacy	FNA	60008	FNA traffic
Legacy	IPX	34837	IPX traffic
Legacy	LAT	60030	LAT traffic
Legacy	MOP-DL	60130	MOP-DL traffic
Legacy	MOP-RC	60131	MOP-RC traffic
Legacy	NETBEUI	60006	NETBEUI traffic
Legacy	PPP	34846	PPP traffic
Legacy	PPPoE	60137	PPPoE traffic
Legacy	SLP	60077	SLP traffic
Legacy	SNA	60007	SNA traffic
Mail	biff	60083	biff traffic
Mail	ccmail	27668	ccmail traffic

Table 2-1 Default applications (continued)

Application group	Sub-components	Value	Description
Mail	ESMTP	5673	ESMTP traffic
Mail	Groupwise	60084	Groupwise traffic
Mail	IMAP	5794	IMAP traffic
Mail	IMAP	5690	IMAP traffic
Mail	IMAP	1009	IMAP traffic
Mail	IMAP	5808	IMAP traffic
Mail	IMAP	5689	IMAP traffic
Mail	Misc-Mail-Port	22079	Misc-Mail-Port traffic
Mail	Misc-Mail-Port	22178	Misc-Mail-Port traffic
Mail	Misc-Mail-Port	22184	Misc-Mail-Port traffic
Mail	Misc-Mail-Port	22551	Misc-Mail-Port traffic
Mail	MSExchange	34817	MSExchange traffic
Mail	MSSQ	60048	MSSQ traffic
Mail	OSI	60071	OSI traffic
Mail	POP	1008	Mail POP3 traffic
Mail	POP	5687	Mail POP3 traffic
Mail	POP-port	22315	POP-port traffic
Mail	pop2	22314	POP2 traffic
Mail	SMTP	5812	Mail SMTP request
Mail	SMTP	5850	Mail SMTP request
Mail	SMTP	1004	Mail SMTP request
Mail	SMTP	5691	Mail SMTP request
Mail	SMTP	5851	Mail SMTP request
Mail	SMTP	5686	Mail SMTP request
Mail	SMTP	5688	Mail SMTP request
Mail	SMTP-port	22080	SMTP-port traffic
Misc	AltaVistaFirewall97	34054	AltaVista Firewall 97 traffic
Misc	AltaVistaFirewall97	34057	AltaVista Firewall 97 traffic
Misc	Anet	34812	Anet traffic
Misc	AppleOUI	34819	AppleOUI traffic
Misc	Appletalk-IP	51326	Appletalk-IP traffic
Misc	Appletalk-IP	51327	Appletalk-IP traffic
Misc	Appletalk-IP	51330	Appletalk-IP traffic
Misc	Appletalk-IP	51329	Appletalk-IP traffic
Misc	Appletalk-IP	51325	Appletalk-IP traffic
Misc	Appletalk-IP	51331	Appletalk-IP traffic

Table 2-1 Default applications (continued)

Application group	Sub-components	Value	Description
Misc	Appletalk-IP	51328	Appletalk-IP traffic
Misc	at-nbp	34813	at-nbp traffic
Misc	Authentication	21140	Authentication traffic
Misc	Authentication	51348	Authentication traffic
Misc	Authentication	51346	Authentication traffic
Misc	Authentication	51343	Authentication traffic
Misc	Authentication	51347	Authentication traffic
Misc	Authentication	21122	Authentication traffic
Misc	bgmp	21470	BGMP traffic
Misc	bootpc	21065	BootPctraffic
Misc	bootps	21064	BootPs traffic
Misc	CHAOSnet	34822	CHAOSnet traffic
Misc	ctf	21116	ctf traffic
Misc	Daynachip	34815	Daynachip traffic
Misc	daytime	20912	daytime traffic
Misc	dcp	21130	dcp traffic
Misc	discard	20909	discard traffic
Misc	DNS	1017	DNS traffic
Misc	dnsix	21125	dnsix traffic
Misc	domain	21036	domain traffic
Misc	dsp	21003	dsp traffic
Misc	dsp3270	34816	dsp3270 traffic
Misc	echo	20908	echo traffic
Misc	finger	21081	Finger traffic
Misc	giop	39042	giop traffic
Misc	giop	39043	giop traffic
Misc	gopher	21069	Gopher traffic
Misc	GSM	34830	GSM traffic
Misc	GSS-SPNEGO	5861	GSS-SPNEGO traffic
Misc	hostname	21147	hostname traffic
Misc	Hosts2-Ns	34804	Hosts2-Ns traffic
Misc	Ingres	34805	Ingres traffic
Misc	IPIX	34826	IPIX traffic
Misc	IPv4	34844	IPv4 traffic
Misc	IPv6	34845	IPv6 traffic
Misc	JPEG	34840	JPEG traffic

Table 2-1 Default applications (continued)

Application group	Sub-components	Value	Description
Misc	Kerberos	34810	Kerberos traffic
Misc	Kerberos	21624	Kerberos traffic
Misc	linuxconf	21139	linuxconf traffic
Misc	LotusNotes	34732	LotusNotes traffic
Misc	ManagementServices	34564	ManagementServices traffic
Misc	ManagementServices	34556	ManagementServices traffic
Misc	ManagementServices	34636	ManagementServices traffic
Misc	ManagementServices	34213	ManagementServices traffic
Misc	ManagementServices	34221	ManagementServices traffic
Misc	ManagementServices	34560	ManagementServices traffic
Misc	ManagementServices	34735	ManagementServices traffic
Misc	ManagementServices	34563	ManagementServices traffic
Misc	ManagementServices	34216	ManagementServices traffic
Misc	Marimba	60015	Marimba traffic
Misc	metagram	21141	metagram traffic
Misc	mfcobol	34209	mfcobol traffic
Misc	Misc-Ports	21070	Misc-Ports traffic
Misc	Misc-Ports	21071	Misc-Ports traffic
Misc	Misc-Ports	21074	Misc-Ports traffic
Misc	Misc-Ports	21043	Misc-Ports traffic
Misc	Misc-Ports	21035	Misc-Ports traffic
Misc	Misc-Ports	21021	Misc-Ports traffic
Misc	Misc-Ports	21302	Misc-Ports traffic
Misc	Misc-Ports	21301	Misc-Ports traffic
Misc	Misc-Ports	21073	Misc-Ports traffic
Misc	Misc-Ports	21072	Misc-Ports traffic
Misc	Misc-Ports	50643	Misc-Ports traffic
Misc	Misc-Ports	37305	Misc-Ports traffic
Misc	Misc-Ports	50795	Misc-Ports traffic
Misc	Misc-Ports	21008	Misc-Ports traffic
Misc	Misc-Ports	21148	Misc-Ports traffic
Misc	Misc-Ports	21121	Misc-Ports traffic
Misc	Misc-Ports	21303	Misc-Ports traffic
Misc	MiscApplication	34847	MiscApplication traffic
Misc	MiscProtocol	34848	MiscProtocol traffic
Misc	MITMLDevice	34208	MITML Device traffic

Table 2-1 Default applications (continued)

Application group	Sub-components	Value	Description
Misc	MITMLDevice	34205	MITML Device traffic
Misc	mpm	21020	mpm traffic
Misc	MSGICP	20996	MSGICP traffic
Misc	msp	20916	msp traffic
Misc	mtp	22177	mtp traffic
Misc	name	21015	name traffic
Misc	Nessus	34731	Nessus traffic
Misc	netstat	20913	netstat traffic
Misc	npp	51324	npp traffic
Misc	NSP	34842	NSP traffic
Misc	nsrmp	34728	nsrmp traffic
Misc	nsrmp	34727	nsrmp traffic
Misc	nsrmp	34661	nsrmp traffic
Misc	NTP	1016	NTP traffic
Misc	NTP	34811	NTP traffic
Misc	ntp	21200	ntp traffic
Misc	objcall	34557	objcall traffic
Misc	qmtp	22550	qmtp traffic
Misc	qotd	20915	qotd traffic
Misc	rap	21007	rap traffic
Misc	RMC	22158	RMC traffic
Misc	RPC	21167	RPC traffic
Misc	snagas	21160	snagas traffic
Misc	snmp	21299	snmp traffic
Misc	snmptrap	21300	snmptrap traffic
Misc	SymantecGhost	34729	Symantec Ghost traffic
Misc	Syslog	1015	Syslog traffic
Misc	time	21006	time traffic
Misc	tlisrv	37309	tlisrv traffic
Misc	ttc	39044	ttc traffic
Misc	ttc	40380	ttc traffic
Misc	ttc	42060	ttc traffic
Misc	Unknown_TCP	34803	Unknown TCP traffic
Misc	Unknown_UDP	34809	Unknown UDP traffic
Misc	UPnP	1018	UPnP traffic
Misc	VMTP	34839	VMTP traffic

Table 2-1 Default applications (continued)

Application group	Sub-components	Value	Description
Misc	whois	21016	whois traffic
Misc	whoisplus	21056	whoisplus traffic
Misc	XNS	21042	XNS traffic
Misc	XNS	21039	XNS traffic
Multimedia	Intellex	6000	Intellex traffic
Multimedia	VideoFrame	60091	VideoFrame traffic
Multimedia	WebEx	60139	WebEx traffic
NetworkManagement	CiscoDiscovery	60055	CiscoDiscovery traffic
NetworkManagement	FlowRecords	60176	Flow records traffic
NetworkManagement	ICMP	60009	ICMP traffic
NetworkManagement	IPComp	60161	IPComp traffic
NetworkManagement	NetFlowV5	60175	NetFlow v5 traffic
NetworkManagement	QFlow Collector	51333	QFlow Collectorr traffic
NetworkManagement	RSVP	60096	RSVP traffic
NetworkManagement	SMS	60087	SMS traffic
NetworkManagement	TimeServer	60125	TimeServer traffic
NetworkManagement	VIPC	34802	VIPC traffic
P2P	Aimster	60132	Aimster traffic
P2P	Audiogalaxy	60118	Audiogalaxy traffic
P2P	BitTorrent	2006	BitTorrent traffic
P2P	Blubster	2003	Blubster traffic
P2P	Common-P2P-Port	33955	Common P2P port traffic
P2P	DirectConnect	5864	DirectConnect traffic
P2P	DirectConnect	5865	DirectConnect traffic
P2P	DirectConnect	5866	DirectConnect traffic
P2P	DirectConnect	5867	DirectConnect traffic
P2P	DirectConnect	5863	DirectConnect traffic
P2P	EarthStationV	60182	EarthStationV traffic
P2PS	FileRogue	60145	FileRogue traffic
P2P	Filetopia	60168	Filetopia traffic
P2P	Furthurnet	60160	Furthernet traffic
P2P	Gnutella	2000	Gnutella traffic
P2P	Groove	60134	Groove traffic
P2P	Hotline	60136	Hotline traffic
P2P	Kazaa	2001	Kazaa traffic
P2P	LimeWire	2008	LimeWire traffic

Table 2-1 Default applications (continued)

Application group	Sub-components	Value	Description
P2P	Morpheus	2010	Morpheus traffic
P2P	Napster	2011	Napster traffic
P2P	Napster2	60181	Napster2 traffic
P2P	OpenNap	2007	OpenNap traffic
P2P	PeerEnabler	2204	P2P PeerEnabler traffic
P2P	PeerEnabler	2004	P2P PeerEnabler traffic
P2P	Piolet	2005	Piolet traffic
P2P	ScourExchange	60113	ScourExchange traffic
P2P	Soulseek	60184	Soulseek traffic
P2P	Tripnosis	60135	Tripnosis traffic
P2P	eDonkey2000	33954	eDonkey2000 traffic
P2P	eDonkey	2002	eDonkey traffic
P2P	eDonkey2000	33956	eDonkey2000 traffic
P2P	iMesh	60114	iMesh traffic
P2P	Gnucleuslan	2009	GnuCleusLan traffic
RemoteAccess	ATSTCP	60107	ATSTCP traffic
RemoteAccess	Attachmate-GW	60100	Attachmate-GW traffic
RemoteAccess	Citrix	34814	Citrix traffic
RemoteAccess	CitrixICA	5671	Remote Access Citrix ICA Traffic
RemoteAccess	CitrixICA	5670	Remote Access Citrix ICA Traffic
RemoteAccess	CORBA	60043	CORBA traffic
RemoteAccess	DceRPC	100663296	DceRPC traffic
RemoteAccess	DceRPC > DceRPCMapper	101908480	DceRPCMapper traffic
RemoteAccess	DceRPC > MsExchange	101974016	MsExchange traffic
RemoteAccess	DceRPC > MsExchange > Directory	102011648	MsExchange traffic
RemoteAccess	DceRPC > MsExchange > InformationStore	102011904	MsExchange traffic
RemoteAccess	DceRPC > MsExchange > MTA	102012160	MsExchange traffic
RemoteAccess	GoToMyPC	60164	GoToMyPC traffic
RemoteAccess	JavaRMI	60109	Java™ RMI traffic
RemoteAccess	login	60089	login traffic
RemoteAccess	MSTerminalServices	6001	MS terminal services
RemoteAccess	OpenConnect-JCP	60085	OpenConnect-JCP traffic
RemoteAccess	OpenWindows	34807	OpenWindows traffic
RemoteAccess	pcanywhere	50528	PCanywhere application
RemoteAccess	PCAnywhere	20948	PCanywhere application

Table 2-1 Default applications (continued)

Application group	Sub-components	Value	Description
RemoteAccess	Persona	60093	Persona traffic
RemoteAccess	radmin	60177	radmin traffic
RemoteAccess	RDP	60052	RDP traffic
RemoteAccess	RemotelyAnywhere	60188	RemotelyAnywhere traffic
RemoteAccess	rexec	60081	rexec traffic
RemoteAccess	rsh	60128	rsh traffic
RemoteAccess	rsync	60159	rsync traffic
RemoteAccess	rtelnet	42372	rtelnet traffic
RemoteAccess	rwho	60090	rwho traffic
RemoteAccess	SmartSockets	60169	SmartSockets traffic
RemoteAccess	SMTBF	60103	SMTBF traffic
RemoteAccess	SSH	1005	SSH traffic
RemoteAccess	SSH-Ports	20949	SSH-Ports traffic
RemoteAccess	SSH-Ports	20947	SSH-Ports traffic
RemoteAccess	SSL	60001	SSL traffic
RemoteAccess	SSL-Shell	60092	SSL-Shell traffic
RemoteAccess	SunRPC	117440512	SunRPC traffic
RemoteAccess	SunRPC	60027	SunRPC traffic
RemoteAccess	SunRPC > IBM3270Mapper	119275520	SunRPC traffic
RemoteAccess	SunRPC > Mount	119209984	SunRPC traffic
RemoteAccess	SunRPC > NFS	118882304	SunRPC traffic
RemoteAccess	SunRPC > NIS	119406592	SunRPC traffic
RemoteAccess	SunRPC > PcNfsd	119472128	SunRPC traffic
RemoteAccess	SunRPC > PortMapper	5383	SunRPC traffic
RemoteAccess	SunRPC > RjeMapper	119341056	SunRPC traffic
RemoteAccess	SunRPC > Rstat	120848384	SunRPC traffic
RemoteAccess	SunRPC > YpBind	119013376	SunRPC traffic
RemoteAccess	SunRPC > YpServ	118947840	SunRPC traffic
RemoteAccess	SunRPC > YpUpdated	119078912	SunRPC traffic
RemoteAccess	SunRPC > YpXferd	119144448	SunRPC traffic
RemoteAccess	Tacacs	34808	Tacacs traffic
RemoteAccess	Telnet	1000	Telnet traffic
RemoteAccess	Telnet-Port	20950	Telnet-Port traffic
RemoteAccess	Timbuktu	60017	Timbuktu traffic
RemoteAccess	tn3270	60010	tn3270 traffic
RemoteAccess	tn5250	60063	tn5250 traffic

Table 2-1 Default applications (continued)

Application group	Sub-components	Value	Description
RemoteAccess	VNC	1006	VNC traffic
RemoteAccess	XWindows	60050	XWindows traffic
RoutingProtocols	ARP	34820	ARP traffic
RoutingProtocols	AURP	60011	AURP traffic
RoutingProtocols	Banyan-VINES	34838	Banyan-VINES traffic
RoutingProtocols	BGP	60029	BGP traffic
RoutingProtocols	BPDU	34821	BPDU traffic
RoutingProtocols	CBT	60045	CBT traffic
RoutingProtocols	CiscoOUI	34823	CiscoOUI traffic
RoutingProtocols	DRP	60038	DRP traffic
RoutingProtocols	DTP	60192	DTP traffic
RoutingProtocols	EGP	60032	EGP traffic
RoutingProtocols	EIGRP	60065	EIGRP traffic
RoutingProtocols	GatewayRouting	34836	Gateway Routing traffic
RoutingProtocols	IanaProtocol-IP	34835	IanaProtocol-IP traffic
RoutingProtocols	IDP	34825	IDP traffic
RoutingProtocols	IGMP	60041	IGMP traffic
RoutingProtocols	IGP	60098	IGP traffic
RoutingProtocols	OSPF	60031	OSPF traffic
RoutingProtocols	PAgP	60190	PAgP traffic
RoutingProtocols	PIM	60044	PIM traffic
RoutingProtocols	PVSTP	60189	PVSTP traffic
RoutingProtocols	RARP	60047	RARP traffic
RoutingProtocols	RIP	60028	RIP traffic
RoutingProtocols	SpanningTree	60046	Spanning tree traffic
RoutingProtocols	VLAN-Bridge	60191	VLAN-Bridge traffic
RoutingProtocols	VTP	60193	VTP traffic
SecurityProtocol	DPA	60061	DPA traffic
SecurityProtocol	GRE	60033	GRE traffic
SecurityProtocol	IPMobility	60172	IPMobility traffic
SecurityProtocol	IPSec	60037	IPSec traffic
SecurityProtocol	ISAKMP	60080	ISAKMP traffic
SecurityProtocol	L2TP	60026	L2TP traffic
SecurityProtocol	PPTP	60036	PPTP traffic
SecurityProtocol	RC5DES	60067	RC5DES traffic
SecurityProtocol	SOCKS	60079	SOCKS traffic

Table 2-1 Default applications (continued)

Application group	Sub-components	Value	Description
SecurityProtocol	SoftEther	60186	SoftEther traffic
SecurityProtocol	SWIPE	60171	SWIPE traffic
Streaming	Abacast	60174	Abacast traffic
Streaming	H.261	34829	H.261 traffic
Streaming	H.262	34828	H.262 traffic
Streaming	H.263	34827	H.263 traffic
Streaming	MicrosoftMediaServer	4002	Streaming Microsoft Media Server Protocol (MMS) traffic
Streaming	MicrosoftMediaServerStreaming	218103808	Streaming Microsoft Media Server Protocol (MMS) traffic
Streaming	MicrosoftMediaServerStreamingPayload	234881024	Streaming Microsoft Media Server Protocol (MMS) traffic
Streaming	Motion	60185	Motion traffic
Streaming	MPEG-Audio	60053	MPEG-Audio traffic
Streaming	MPEG-Video	60054	MPEG-Video traffic
Streaming	RadioNetscape	60180	RadioNetscape traffic
Streaming	Real	60003	Real traffic
Streaming	RTP-Skinny	34834	RTP-Skinny traffic
Streaming	RTSP	5071	RTSP traffic
Streaming	RTSP > RTSPEmbeddedMedia	187367424	RTSP traffic
Streaming	RTSP > RTSPEmbeddedMedia > RealRDT	187405824	RTSP traffic
Streaming	RTSP > RTSPEmbeddedMedia > RealRDT > RTSPavpaudio	187405832	RTSP traffic
Streaming	RTSP > RTSPEmbeddedMedia > RealRDT > RTSPavpdynamicunknown	187405831	RTSP traffic
Streaming	RTSP > RTSPEmbeddedMedia > RealRDT > RTSPavpreserved	187405830	RTSP traffic
Streaming	RTSP > RTSPEmbeddedMedia > RealRDT > RTSPavpunassigned	187405829	RTSP traffic
Streaming	RTSP > RTSPEmbeddedMedia > RealRDT > RTSPavpvideo	187405833	RTSP traffic
Streaming	RTSP > RTSPEmbeddedMedia > RTCP	187406336	RTSP traffic
Streaming	RTSP > RTSPEmbeddedMedia > RTP	187406080	RTSP traffic
Streaming	RTSP > RTSPEmbeddedMedia > RTP > RTSPavpdynamicunknown	187406087	RTSP traffic
Streaming	RTSP > RTSPEmbeddedMedia > RTP > RTSPavpunassigned	187406085	RTSP traffic

Table 2-1 Default applications (continued)

Application group	Sub-components	Value	Description
Streaming	RTSP > RTSPEmbeddedMedia > RTP > RTSPavpvideo	187406089	RTSP traffic
Streaming	RTSP > RTSPEmbeddedMediaRTP > RTSPavpreserved	187406086	RTSP traffic
Streaming	RTSP > RTSPSessionControl	187301888	RTSP traffic
Streaming	RTSP> RTSPEmbeddedMedia > RTP > RTSPavpaudio	187406088	RTSP traffic
Streaming	ST2	60034	ST2 traffic
Streaming	StreamingAudio	4001	Shoutcast MP3 stream
Streaming	StreamingAudio	4000	Shoutcast MP3 stream
Streaming	StreamWorks	60014	StreamWorks traffic
Streaming	WinampStream	60165	WinampStream traffic
Streaming	WindowsMediaPlayer	5005	WindowsMediaPlayer traffic
Streaming	WindowsMediaPlayer	5006	WindowsMediaPlayer traffic
Streaming	WinMedia	60025	WinMedia traffic
UncommonProtocol	DEC	34824	DEC traffic
UncommonProtocol	UncommonProtocol	34850	UncommonProtocol traffic
VoIP	CiscoCTI	60144	CiscoCTI traffic
VoIP	Clarent-CC	60075	Clarent-CC traffic
VoIP	Clarent-Complex	60074	Clarent-Complex traffic
VoIP	Clarent-Mgmt	60072	Clarent-Mgmt traffic
VoIP	Clarent-Voice-S	60073	Clarent-Voice-S traffic
VoIP	Dialpad	60140	Dialpad traffic
VoIP	G711	34833	G711 traffic
VoIP	G722	34832	G722 traffic
VoIP	G729	34831	G729 traffic
VoIP	H.323	60018	H.323 traffic
VoIP	H323	33554432	H.323 traffic
VoIP	H323 > CallControl	34144256	H.323 traffic
VoIP	H323 > CallControl > H245	34176768	H.323 traffic
VoIP	H323 > CallSignaling	34078720	H.323 traffic
VoIP	H323 > CallSignaling > Q931	34110976	H.323 traffic
VoIP	I-Phone	60066	I-Phone traffic
VoIP	MCK-Signaling	60094	MCK-Signaling traffic
VoIP	MCK-Voice	60095	MCK-Voice traffic
VoIP	Megaco	60155	Megaco traffic
VoIP	MGCP	60152	MGCP traffic

Table 2-1 Default applications (continued)

Application group	Sub-components	Value	Description
VoIP	Micom-VIP	60035	Micom-VIP traffic
VoIP	Net2Phone	60153	Net2Phone traffic
VoIP	RTCP	50331648	RTCP traffic
VoIP	RTCP-B	60022	RTCP-B traffic
VoIP	RTCP-I	60020	RTCP-I traffic
VoIP	RTP	67108864	RTP traffic
VoIP	RTP > H323Audio	67764224	RTP traffic
VoIP	RTP > H323Audio > CN	67799040	RTP traffic
VoIP	RTP > H323Audio > DVI4	67797760	RTP traffic
VoIP	RTP > H323Audio > G711	67796992	RTP traffic
VoIP	RTP > H323Audio > G722	67798272	RTP traffic
VoIP	RTP > H323Audio > G723	67797504	RTP traffic
VoIP	RTP > H323Audio > G728	67799552	RTP traffic
VoIP	RTP > H323Audio > G729	67803904	RTP traffic
VoIP	RTP > H323Audio > GSM	67797248	RTP traffic
VoIP	RTP > H323Audio > L16	67798528	RTP traffic
VoIP	RTP > H323Audio > LPC	67798016	RTP traffic
VoIP	RTP > H323Audio > MPA	67799296	RTP traffic
VoIP	RTP > H323Audio > QCELP	67798784	RTP traffic
VoIP	RTP > H323Video	67829760	RTP traffic
VoIP	RTP > H323Video > CELB	67865600	RTP traffic
VoIP	RTP > H323Video > H263	67867136	RTP traffic
VoIP	RTP > H323Video > JPEG	67865856	RTP traffic
VoIP	RTP > H323Video > MP2T	67866880	RTP traffic
VoIP	RTP > H323Video > MPV	67866624	RTP traffic
VoIP	RTP > H323Video > NV	67866112	RTP traffic
VoIP	RTP > H323Video >H261	67866368	RTP traffic
VoIP	RTP > SIPavpaudio	68157440	RTP traffic
VoIP	RTP > SIPavpdata	68288512	RTP traffic
VoIP	RTP > SIPavpdynamicunknown	68091904	RTP traffic
VoIP	RTP > SIPavpreserved	68026368	RTP traffic
VoIP	RTP > SIPavpunassigned	26796083	RTP traffic
VoIP	RTP > SIPavpvideo	68222976	RTP traffic
VoIP	RTP > SKINNYAudio	70385664	RTP traffic
VoIP	RTP > SKINNYAudio > ActiveVoice	70426624	RTP traffic
VoIP	RTP > SKINNYAudio > G711	70418432	RTP traffic

Table 2-1 Default applications (continued)

Application group	Sub-components	Value	Description
VoIP	RTP > SKINNYAudio > G711 > aLaw56k	70418443	RTP traffic
VoIP	RTP > SKINNYAudio > G711 > aLaw64k	70418442	RTP traffic
VoIP	RTP > SKINNYAudio > G711 > uLaw56k	70418445	RTP traffic
VoIP	RTP > SKINNYAudio > G711 > uLaw64k	70418444	RTP traffic
VoIP	RTP > SKINNYAudio > G722	70419712	RTP traffic
VoIP	RTP > SKINNYAudio > G722 > 48k	70419728	RTP traffic
VoIP	RTP > SKINNYAudio > G722 > 56k	70419727	RTP traffic
VoIP	RTP > SKINNYAudio > G722 > 64k	70419726	RTP traffic
VoIP	RTP > SKINNYAudio > G7231	70425088	RTP traffic
VoIP	RTP > SKINNYAudio > G72616k	70425856	RTP traffic
VoIP	RTP > SKINNYAudio > G72624k	70426112	RTP traffic
VoIP	RTP > SKINNYAudio > G72632k	70426368	RTP traffic
VoIP	RTP > SKINNYAudio > G728	70420992	RTP traffic
VoIP	RTP > SKINNYAudio > G729	70425344	RTP traffic
VoIP	RTP > SKINNYAudio > G729 > AnnexA	70425361	RTP traffic
VoIP	RTP > SKINNYAudio > G729 > AnnexAB	70425363	RTP traffic
VoIP	RTP > SKINNYAudio > G729 > AnnexB	70425362	RTP traffic
VoIP	RTP > SKINNYAudio > GSM	70418688	RTP traffic
VoIP	RTP > SKINNYAudio > GSM > ENHRate	70418712	RTP traffic
VoIP	RTP > SKINNYAudio > GSM > FullRate	70418710	RTP traffic
VoIP	RTP > SKINNYAudio > GSM > HalfRate	70418711	RTP traffic
VoIP	RTP > SKINNYAudio > GSM > STDRate	70418713	RTP traffic
VoIP	RTP > SKINNYAudio > WideBand	70425600	RTP traffic
VoIP	RTP > SKINNYAudio > WideBand > 256k	70425626	RTP traffic
VoIP	RTP > SKINNYAudio> G729 > G729B	70425364	RTP traffic
VoIP	RTP > SKINNYData	70451200	RTP traffic
VoIP	RTP > SKINNYData > 56k	70492672	RTP traffic
VoIP	RTP > SKINNYDate > 64k	70492416	RTP traffic
VoIP	RTP > SKINNYNonStd	70320128	RTP traffic
VoIP	RTP-B	60021	RTP traffic
VoIP	RTP-I	60019	RTP traffic

Table 2-1 Default applications (continued)

Application group	Sub-components	Value	Description
VoIP	SCCP	352321536	SCCP traffic
VoIP	SIP	60151	SIP traffic
VoIP	SIP > SipSessionControl	84672512	SIP traffic
VoIP	Skype	452984832	Skype traffic
VoIP	Skype	3007	Skype traffic
VoIP	T.120	60023	T.120 traffic
VoIP	VDOPhone	60004	VDOPhone traffic
VoIP	Vonage	60187	Vonage traffic
Web		16777216	Web traffic
Web	Application	16908288	Web Application traffic
Web	Application > ATTA2BMusic	16926208	ATTA2BMusic traffic
Web	Application > Backweb	16909568	Backweb traffic
Web	Application > Datawindow	16909824	Datawindow traffic
Web	Application > Edact	16910592	Edact traffic
Web	Application > EdiContent	16910080	EdiContent traffic
Web	Application > EdiX12	16910336	EdiX12 traffic
Web	Application > Entrypoint	16909312	Entrypoint traffic
Web	Application > Excel	16910848	Excel traffic
Web	Application > FutureSplash	16927232	FutureSplash traffic
Web	Application > MACBINHEX40	16911104	MACBINHEX40 traffic
Web	Application > MARIMBA	16924672	MARIMBA traffic
Web	Application > MP3	16911360	MP3 traffic
Web	Application > MsPowerPoint	16911616	MsPowerPoint traffic
Web	Application > MsWord	16911872	MsWord traffic
Web	Application > NewsMessageID	16912128	NewsMessageID traffic
Web	Application > NewsTransmission	16912384	NewsTransmission traffic
Web	Application > OctetStream	16912640	OctetStream traffic
Web	Application > ODA	16912896	ODA traffic
Web	Application > PDF	16913152	PDF traffic
Web	Application > PostScript	16913408	PostScript traffic
Web	Application > PowerBuilder	16913664	PowerBuilder traffic
Web	Application > QuattroPro	16913920	QuattroPro traffic
Web	Application > RTF	16914176	RTF traffic
Web	Application > SDP	16926720	SDP traffic
Web	Application > SGML	16914432	SGML traffic
Web	Application > ShockWaveFlash	16926976	ShockWaveFlash traffic

Table 2-1 Default applications (continued)

Application group	Sub-components	Value	Description
Web	Application > VNDFrameMaker	16914688	VNDFrameMaker traffic
Web	Application > VNDLotusFreeLance	16915200	VNDLotusFreeLance traffic
Web	Application > VNDLotusOTUS123	16914944	VNDLotusOTUS123 traffic
Web	Application > VNDLOTUSWordPro	16915456	VNDLOTUSWordPro traffic
Web	Application > VNDM	16915712	VNDM traffic
Web	Application > VNDMsExcel	16915968	VNDMsExcel traffic
Web	Application > VNDMsPowerPoint	16916224	VNDMsPowerPoint traffic
Web	Application > VNDMsProject	16916480	VNDMsProject traffic
Web	Application > VNDMsWord	16916736	VNDMsWord traffic
Web	Application > VNDPowerBuilder	16916992	VNDPowerBuilder traffic
Web	Application > VNDRNMusicPackage	16926464	VNDRNMusicPackage traffic
Web	Application > VNDRNRealPlayer	16917248	VNDRNRealPlayer traffic
Web	Application > VNDVisio	16917504	VNDVisio traffic
Web	Application > WordPerfect	16917760	WordPerfect traffic
Web	Application > X_NETCDF	16924416	X_NETCDF traffic
Web	Application > XBCPIO	16918016	XBCPIO traffic
Web	Application > XCOMPRESS	16918272	XCOMPRESS traffic
Web	Application > XCPIO	16918528	XCPIO traffic
Web	Application > XCSH	16918784	XCSH traffic
Web	Application > XDIRECTOR	16919040	XDIRECTOR traffic
Web	Application > XDVI	16919296	XDVI traffic
Web	Application > XGTAR	16919552	XGTAR traffic
Web	Application > XIPIX	16925952	XIPIX traffic
Web	Application > XIpScript	16925696	XIpScript traffic
Web	Application > XJAVASCRIPT	16919808	XJAVASCRIPT traffic
Web	Application > XLATEX	16920064	XLATEX traffic
Web	Application > XLiquidPlayer	16925440	XLiquidPlayer traffic
Web	Application > XLotusNotes	16920320	XLotusNotes traffic
Web	Application > XM	16920832	XM traffic
Web	Application > XMACBinary	16920576	XMACBinary traffic
Web	Application > XPNCMD	16921088	XPNCMD traffic
Web	Application > XPNRealAudio	16921344	XPNRealAudio traffic
Web	Application > XPowerPoint	16921600	XPowerPoint traffic
Web	Application > XPP5	16923904	XPP5 traffic
Web	Application > XSH(53)	16921856	XSH(53) traffic
Web	Application > XSTUFFIT	16922112	XSTUFFIT traffic

Table 2-1 Default applications (continued)

Application group	Sub-components	Value	Description
Web	Application > XTAR	16922368	XTAR traffic
Web	Application > XTCL	16922624	XTCL traffic
Web	Application > XTEX	16922880	XTEX traffic
Web	Application > XTROFF	16923136	XTROFF traffic
Web	Application > XUSTAR	16923392	XUSTAR traffic
Web	Application > XXDMA	16924928	XXDMA traffic
Web	Application > XXSM	16925184	XXSM traffic
Web	Application > XZipCompressed	16923648	XZipCompressed traffic
Web	Application > ZIPARCHIVE	16924160	ZIPARCHIVE traffic
Web	Audio	16973824	Web Audio traffic
Web	Audio > BC	16993024	BC traffic
Web	Audio > MIDI	16993280	MIDI traffic
Web	Audio > MPEG	16993536	MPEG traffic
Web	Audio > VNDRNRealAudio	16993792	VNDRNRealAudio traffic
Web	Audio > WAV	16994048	WAV traffic
Web	Audio > XAF	16994304	XAF traffic
Web	Audio > XLIQUID(86)	16995840	XLIQUID(86) traffic
Web	Audio > XMIDI	16994560	XMIDI traffic
Web	Audio > XMPEG	16994816	XMPEG traffic
Web	Audio > XMPGURL	16995072	XMPGURL traffic
Web	Audio > XWAV(85)	16995584	XWAV(85) traffic
Web	Blogs	16777269	Blogs traffic
Web	Blogs > Application	16908341	Blogs traffic
Web	Blogs > Audio	16973877	Blogs traffic
Web	Blogs > Database	16842805	Blogs traffic
Web	Blogs > Image	17039413	Blogs traffic
Web	Blogs > Text	17104949	Blogs traffic
Web	Blogs > Video	17170485	Blogs traffic
Web	Blogs > XWORLD	17236021	Blogs traffic
Web	Database	16842752	Web database traffic
Web	Database > JDBC	16843520	JDBC traffic
Web	Database > SybaseTunneledTDS	16843264	SybaseTunneledTDS traffic
Web	Database > SybaseWebSQL	16843008	SybaseWebSQL traffic
Web	Facebook	16777246	Facebook traffic
Web	Facebook > Application	16908318	Facebook traffic
Web	Facebook > Audio	16973854	Facebook traffic

Table 2-1 Default applications (continued)

Application group	Sub-components	Value	Description
Web	Facebook > Database	16842782	Facebook traffic
Web	Facebook > Image	17039390	Facebook traffic
Web	Facebook > Text	17104926	Facebook traffic
Web	Facebook > Video	17170462	Facebook traffic
Web	Facebook > XWORLD	17235998	Facebook traffic
Web	FileSharingSites	16777440	File sharing site traffic
Web	FileSharingSites > Application	16908512	File sharing site traffic
Web	FileSharingSites > Audio	16974048	File sharing site traffic
Web	FileSharingSites > Database	16842976	File sharing site traffic
Web	FileSharingSites > Image	17039584	File sharing site traffic
Web	FileSharingSites > Text	17105120	File sharing site traffic
Web	FileSharingSites > Video	17170656	File sharing site traffic
Web	FileSharingSites > XWORLD	17236192	File sharing site traffic
Web	FreeEmailSites	16777441	Free email site traffic
Web	FreeEmailSites > Application	16908513	Free email site traffic
Web	FreeEmailSites > Audio	16974049	Free email site traffic
Web	FreeEmailSites > Database	16842977	Free email site traffic
Web	FreeEmailSites > Image	17039585	Free email site traffic
Web	FreeEmailSites > Text	17105121	Free email site traffic
Web	FreeEmailSites > Video	17170657	Free email site traffic
Web	FreeEmailSites > XWORLD	17236193	Free email site traffic
Web	Google	16777245	Google traffic
Web	Google > Application	16908317	Google traffic
Web	Google > Audio	16973853	Google traffic
Web	Google > Database	16842781	Google traffic
Web	Google > Image	17039389	Google traffic
Web	Google > Text	17104925	Google traffic
Web	Google > Video	17170461	Google traffic
Web	Google > XWORLD	17235997	Google traffic
Web	http(8080)	21085	http(8080) traffic
Web	http(81)	21109	http(81) traffic
Web	HTTPImageTransfer	1034	HTTPImageTransfer traffic
Web	Image	17039360	Web image traffic
Web	Image > CGM	17061632	CGM traffic
Web	Image > G3FAX	17061888	G3FAX traffic
Web	Image > GIF	17062144	GIF traffic

Table 2-1 Default applications (continued)

Application group	Sub-components	Value	Description
Web	Image > IEF	17062400	IEF traffic
Web	Image > JPEG	17062656	JPEG traffic
Web	Image > PICT	17062912	PICT traffic
Web	Image > PNG	17063168	PNG traffic
Web	Image > TF	17063424	TF traffic
Web	Image > VNDRNRealFlash	17063680	VNDRNRealFlash traffic
Web	Image > VNDRNRealPix	17063936	VNDRNRealPix traffic
Web	Image > XBitAppNames	17064192	XBitAppNames traffic
Web	Image > XPixAppNames	17064448	XPixAppNames traffic
Web	Image > XQuickTime	17064704	XQuickTime traffic
Web	Image > XWindowDump	17064960	XWindowDump traffic
Web	Image > XXBM	17065216	XXBM traffic
Web	Info	16777268	Info traffic
Web	Info > Application	16908340	Info traffic
Web	Info > Audio	16973876	Info traffic
Web	Info > Database	16842804	Info traffic
Web	Info > Image	17039412	Info traffic
Web	Info > Text	17104948	Info traffic
Web	Info > Video	17170484	Info traffic
Web	Info > XWORLD	17236020	Info traffic
Web	JAVA	5050	JAVA™ traffic
Web	Malware(attack)	16777424	Malware (attack)traffic
Web	Malware(attack) > Application	16908496	Malware (attack)traffic
Web	Malware(attack) > Audio	16974032	Malware (attack)traffic
Web	Malware(attack) > Database	16842960	Malware (attack)traffic
Web	Malware(attack) > Image	17039568	Malware (attack)traffic
Web	Malware(attack) > Text	17105104	Malware (attack)traffic
Web	Malware(attack) > Video	17170640	Malware (attack)traffic
Web	Malware(attack) > XWORLD	17236176	Malware (attack)traffic
Web	Malware(backdoor)	16777428	Malware (backdoor) traffic
Web	Malware(backdoor) > Application	16908500	Malware (backdoor) traffic
Web	Malware(backdoor) > Audio	16974036	Malware (backdoor) traffic
Web	Malware(backdoor) > Database	16842964	Malware (backdoor) traffic
Web	Malware(backdoor) > Image	17039572	Malware (backdoor) traffic
Web	Malware(backdoor) > Text	17105108	Malware (backdoor) traffic
Web	Malware(backdoor) > Video	17170644	Malware (backdoor) traffic

Table 2-1 Default applications (continued)

Application group	Sub-components	Value	Description
Web	Malware(backdoor) > XWORLD	17236180	Malware (backdoor) traffic
Web	Malware(blacklist)	16777426	Malware (blacklist) traffic
Web	Malware(blacklist) > Application	16908498	Malware (blacklist) traffic
Web	Malware(blacklist) > Audio	16974034	Malware (blacklist) traffic
Web	Malware(blacklist) > Database	16842962	Malware (blacklist) traffic
Web	Malware(blacklist) > Image	17039570	Malware (blacklist) traffic
Web	Malware(blacklist) > Text	17105106	Malware (blacklist) traffic
Web	Malware(blacklist) > Video	17170642	Malware (blacklist) traffic
Web	Malware(blacklist) > XWORLD	17236178	Malware (blacklist) traffic
Web	Malware(bot)	16777417	Malware (bot) traffic
Web	Malware(bot) > Application	16908489	Malware (bot) traffic
Web	Malware(bot) > Audio	16974025	Malware (bot) traffic
Web	Malware(bot) > Database	16842953	Malware (bot) traffic
Web	Malware(bot) > Image	17039561	Malware (bot) traffic
Web	Malware(bot) > Text#	17105097	Malware (bot) traffic
Web	Malware(bot) > Video	17170633	Malware (bot) traffic
Web	Malware(bot) > XWORLD	17236169	Malware (bot) traffic
Web	Malware(exploit)	16777419	Malware (exploit) traffic
Web	Malware(exploit) > Application	16908491	Malware (exploit) traffic
Web	Malware(exploit) > Audio	16974027	Malware (exploit) traffic
Web	Malware(exploit) > Database	16842955	Malware (exploit) traffic
Web	Malware(exploit) > Image	17039563	Malware (exploit) traffic
Web	Malware(exploit) > Text	17105099	Malware (exploit) traffic
Web	Malware(exploit) > Video	17170635	Malware (exploit) traffic
Web	Malware(exploit) > XWORLD	17236171	Malware (exploit) traffic
Web	Malware(flux > Audio	16974033	Malware (flux) traffic
Web	Malware(flux)	16777425	Malware (flux) traffic
Web	Malware(flux) > Application	16908497	Malware (flux) traffic
Web	Malware(flux) > Database	16842961	Malware (flux) traffic
Web	Malware(flux) > Image	17039569	Malware (flux) traffic
Web	Malware(flux) > Text	17105105	Malware (flux) traffic
Web	Malware(flux) > Video	17170641	Malware (flux) traffic
Web	Malware(flux) > XWORLD	17236177	Malware (flux) traffic
Web	Malware(fraud)	16777421	Malware (fraud) traffic
Web	Malware(fraud) > Application	16908493	Malware (fraud) traffic
Web	Malware(fraud) > Audio	16974029	Malware (fraud) traffic

Table 2-1 Default applications (continued)

Application group	Sub-components	Value	Description
Web	Malware(fraud) > Database	16842957	Malware (fraud) traffic
Web	Malware(fraud) > Image	17039565	Malware (fraud) traffic
Web	Malware(fraud) > Text	17105101	Malware (fraud) traffic
Web	Malware(fraud) > Video	17170637	Malware (fraud) traffic
Web	Malware(fraud) > XWORLD	17236173	Malware (fraud) traffic
Web	Malware(hack)	16777420	Malware (hack) traffic
Web	Malware(hack) > Application	16908492	Malware (hack) traffic
Web	Malware(hack) > Audio	16974028	Malware (hack) traffic
Web	Malware(hack) > Database	16842956	Malware (hack) traffic
Web	Malware(hack) > Image	17039564	Malware (hack) traffic
Web	Malware(hack) > Text	17105100	Malware (hack) traffic
Web	Malware(hack) > Video	17170636	Malware(hack) traffic
Web	Malware(hack) > XWORLD	17236172	Malware (hack) traffic
Web	Malware(misc)	16777416	Malware (misc) traffic
Web	Malware(misc) > Application	16908488	Malware (misc) traffic
Web	Malware(misc) > Audio	16974024	Malware (misc) traffic
Web	Malware(misc) > Database	16842952	Malware (misc) traffic
Web	Malware(misc) > Image	17039560	Malware (misc) traffic
Web	Malware(misc) > Text	17105096	Malware (misc) traffic
Web	Malware(misc) > Video	17170632	Malware (misc) traffic
Web	Malware(misc) > XWORLD	17236168	Malware (misc) traffic
Web	Malware(phish)	16777422	Malware (phish) traffic
Web	Malware(phish) > Application	16908494	Malware (phish) traffic
Web	Malware(phish) > Audio	16974030	Malware (phish) traffic
Web	Malware(phish) > Database	16842958	Malware (phish) traffic
Web	Malware(phish) > Image	17039566	Malware (phish) traffic
Web	Malware(phish) > Text	17105102	Malware (phish) traffic
Web	Malware(phish) > Video	17170638	Malware (phish) traffic
Web	Malware(phish) > XWORLD	17236174	Malware (phish) traffic
Web	Malware(rbn)	16777430	Malware (rbn) traffic
Web	Malware(rbn) > Application	16908502	Malware (rbn) traffic
Web	Malware(rbn) > Audio	16974038	Malware (rbn) traffic
Web	Malware(rbn) > Database	16842966	Malware (rbn) traffic
Web	Malware(rbn) > Image	17039574	Malware (rbn) traffic
Web	Malware(rbn) > Text#	17105110	Malware (rbn) traffic
Web	Malware(rbn) > Video	17170646	Malware (rbn) traffic

Table 2-1 Default applications (continued)

Application group	Sub-components	Value	Description
Web	Malware(rbn) > XWORLD	17236182	Malware (rbn) traffic
Web	Malware(rogue)	31677742	Malware (rogue) traffic
Web	Malware(rogue) > Application	16908495	Malware (rogue) traffic
Web	Malware(rogue) > Audio	16974031	Malware (rogue) traffic
Web	Malware(rogue) > Database	16842959	Malware (rogue) traffic
Web	Malware(rogue) > Image	17039567	Malware (rogue) traffic
Web	Malware(rogue) > Text	17105103	Malware (rogue) traffic
Web	Malware(rogue) > Video	17170639	Malware (rogue) traffic
Web	Malware(rogue) > XWORLD	17236175	Malware (rogue) traffic
Web	Malware(sql > Application	16908499	Malware (sql) traffic
Web	Malware(sql)	16777427	Malware (sql) traffic
Web	Malware(sql) > Audio	16974035	Malware (sql) traffic
Web	Malware(sql) > Database	16842963	Malware (sql) traffic
Web	Malware(sql) > Image	17039571	Malware (sql) traffic
Web	Malware(sql) > Text	17105107	Malware (sql) traffic
Web	Malware(sql) > Video	17170643	Malware (sql) traffic
Web	Malware(sql) > XWORLD	17236179	Malware (sql) traffic
Web	Malware(suspicious)	16777429	Malware (suspicious) traffic
Web	Malware(suspicious) > Application	16908501	Malware (suspicious) traffic
Web	Malware(suspicious) > Audio	16974037	Malware (suspicious) traffic
Web	Malware(suspicious) > Database	16842965	Malware (suspicious) traffic
Web	Malware(suspicious) > Image	17039573	Malware (suspicious) traffic
Web	Malware(suspicious) > Text	17105109	Malware (suspicious) traffic
Web	Malware(suspicious) > Video	17170645	Malware (suspicious) traffic
Web	Malware(suspicious) > XWORLD	17236181	Malware (suspicious) traffic
Web	Malware(trojan)	16777418	Malware (trojan) traffic
Web	Malware(trojan) > Application	16908490	Malware (trojan) traffic
Web	Malware(trojan) > Audio	16974026	Malware (trojan) traffic
Web	Malware(trojan) > Database	16842954	Malware (trojan) traffic
Web	Malware(trojan) > Image	17039562	Malware (trojan) traffic
Web	Malware(trojan) > Text	17105098	Malware (trojan) traffic
Web	Malware(trojan) > Video	17170634	Malware (trojan) traffic
Web	Malware(trojan) > XWORLD	17236170	Malware (trojan) traffic
Web	MSNLive	16777248	MSNLive traffic
Web	MSNLive > Application	16908320	MSNLive traffic
Web	MSNLive > Audio	16973856	MSNLive traffic

Table 2-1 Default applications (continued)

Application group	Sub-components	Value	Description
Web	MSNLive > Database	16842784	MSNLive traffic
Web	MSNLive > Image	17039392	MSNLive traffic
Web	MSNLive > Text	17104928	MSNLive traffic
Web	MSNLive > Video	17170464	MSNLive traffic
Web	MSNLive > XWORLD	17236000	MSNLive traffic
Web	NortonAntiVirus	1025	NortonAntiVirus traffic
Web	SecureWeb	1011	SecureWeb traffic
Web	Shopping	16777267	Shopping traffic
Web	Shopping > Application	16908339	Shopping traffic
Web	Shopping > Audio	16973875	Shopping traffic
Web	Shopping > Database	16842803	Shopping traffic
Web	Shopping > Image	17039411	Shopping traffic
Web	Shopping > Text	17104947	Shopping traffic
Web	Shopping > Video	17170483	Shopping traffic
Web	Shopping > XWORLD	17236019	Shopping traffic
Web	SocialNetwork > ADULTFRIENDFINDER	16777255	Adult FriendFinder traffic
Web	SocialNetwork > ADULTFRIENDFINDER > Application	16908327	Adult FriendFinder traffic
Web	SocialNetwork > ADULTFRIENDFINDER > Audio	16973863	Adult FriendFinder traffic
Web	SocialNetwork > ADULTFRIENDFINDER > Database	16842791	Adult FriendFinder traffic
Web	SocialNetwork > ADULTFRIENDFINDER > Image	17039399	Adult FriendFinder traffic
Web	SocialNetwork > ADULTFRIENDFINDER > Text	17104935	Adult FriendFinder traffic
Web	SocialNetwork > ADULTFRIENDFINDER > Video	17170471	Adult FriendFinder traffic
Web	SocialNetwork > ADULTFRIENDFINDER > XWORLD	17236007	Adult FriendFinder traffic
Web	SocialNetwork > BLOGSTER	16777256	Blogster traffic
Web	SocialNetwork > BLOGSTER > Application	16908328	Blogster traffic
Web	SocialNetwork > BLOGSTER > Audio	16973864	Blogster traffic
Web	SocialNetwork > BLOGSTER > Database	16842792	Blogster traffic
Web	SocialNetwork > BLOGSTER > Image	17039400	Blogster traffic
Web	SocialNetwork > BLOGSTER > Text	17104936	Blogster traffic

Table 2-1 Default applications (continued)

Application group	Sub-components	Value	Description
Web	SocialNetwork > BLOGSTER > Video	17170472	Blogster traffic
Web	SocialNetwork > BLOGSTER > XWORLD	17236008	Blogster traffic
Web	SocialNetwork > CLASSMATES	16777264	Classmates traffic
Web	SocialNetwork > CLASSMATES > Application	16908336	Classmates traffic
Web	SocialNetwork > CLASSMATES > Audio	16973872	Classmates traffic
Web	SocialNetwork > CLASSMATES > Database	16842800	Classmates traffic
Web	SocialNetwork > CLASSMATES > Image	17039408	Classmates traffic
Web	SocialNetwork > CLASSMATES > Text	17104944	Classmates traffic
Web	SocialNetwork > CLASSMATES > Video	17170480	Classmates traffic
Web	SocialNetwork > CLASSMATES > XWORLD	17236016	Classmates traffic
Web	SocialNetwork > FLICKR	16777250	Flickr traffic
Web	SocialNetwork > FLICKR > Application	16908322	Flickr traffic
Web	SocialNetwork > FLICKR > Audio	16973858	Flickr traffic
Web	SocialNetwork > FLICKR > Database	16842786	Flickr traffic
Web	SocialNetwork > FLICKR > Image	17039394	Flickr traffic
Web	SocialNetwork > FLICKR > Text	17104930	Flickr traffic
Web	SocialNetwork > FLICKR > Video	17170466	Flickr traffic
Web	SocialNetwork > FLICKR > XWORLD	17236002	Flickr traffic
Web	SocialNetwork > FRIENDSTER	16777257	Friendster traffic
Web	SocialNetwork > FRIENDSTER > Application	16908329	Friendster traffic
Web	SocialNetwork > FRIENDSTER > Audio	16973865	Friendster traffic
Web	SocialNetwork > FRIENDSTER > Database	16842793	Friendster traffic
Web	SocialNetwork > FRIENDSTER > Image	17039401	Friendster traffic
Web	SocialNetwork > FRIENDSTER > Text	17104937	Friendster traffic
Web	SocialNetwork > FRIENDSTER > Video	17170473	Friendster traffic
Web	SocialNetwork > FRIENDSTER > XWORLD	17236009	Friendster traffic
Web	SocialNetwork > HI5	16777258	Hi5 traffic
Web	SocialNetwork > HI5 > Application	16908330	Hi5 traffic
Web	SocialNetwork > HI5 > Audio	16973866	Hi5 traffic
Web	SocialNetwork > HI5 > Database	16842794	Hi5 traffic

Table 2-1 Default applications (continued)

Application group	Sub-components	Value	Description
Web	SocialNetwork > HI5 > Image	17039402	Hi5 traffic
Web	SocialNetwork > HI5 > Text	17104938	Hi5 traffic
Web	SocialNetwork > HI5 > Video	17170474	Hi5 traffic
Web	SocialNetwork > HI5 > XWORLD	17236010	Hi5 traffic
Web	SocialNetwork > JAIKU	16777259	Jaiku traffic
Web	SocialNetwork > JAIKU > Application	16908331	Jaiku traffic
Web	SocialNetwork > JAIKU > Audio	16973867	Jaiku traffic
Web	SocialNetwork > JAIKU > Database	16842795	Jaiku traffic
Web	SocialNetwork > JAIKU > Image	31703940	Jaiku traffic
Web	SocialNetwork > JAIKU > Text	17104939	Jaiku traffic
Web	SocialNetwork > JAIKU > Video	17170475	Jaiku traffic
Web	SocialNetwork > JAIKU > XWORLD	17236011	Jaiku traffic
Web	SocialNetwork > KAIXIN	16777260	Kaixin traffic
Web	SocialNetwork > KAIXIN > Application	16908332	Kaixin traffic
Web	SocialNetwork > KAIXIN > Audio	16973868	Kaixin traffic
Web	SocialNetwork > KAIXIN > Database	16842796	Kaixin traffic
Web	SocialNetwork > KAIXIN > Image	17039404	Kaixin traffic
Web	SocialNetwork > KAIXIN > Text	17104940	Kaixin traffic
Web	SocialNetwork > KAIXIN > Video	17170476	Kaixin traffic
Web	SocialNetwork > KAIXIN > XWORLD	17236012	Kaixin traffic
Web	SocialNetwork > LINKEDIN	16777249	LinkedIn traffic
Web	SocialNetwork > LINKEDIN > Application	16908321	LinkedIn traffic
Web	SocialNetwork > LINKEDIN > Audio	16973857	LinkedIn traffic
Web	SocialNetwork > LINKEDIN > Database	16842785	LinkedIn traffic
Web	SocialNetwork > LINKEDIN > Image	17039393	LinkedIn traffic
Web	SocialNetwork > LINKEDIN > Text	17104929	LinkedIn traffic
Web	SocialNetwork > LINKEDIN > Video	17170465	LinkedIn traffic
Web	SocialNetwork > LINKEDIN > XWORLD	17236001	LinkedIn traffic
Web	SocialNetwork > MIXI	16777254	mixi traffic
Web	SocialNetwork > MIXI > Application	16908326	mixi traffic
Web	SocialNetwork > MIXI > Audio	16973862	mixi traffic
Web	SocialNetwork > MIXI > Database	16842790	mixi traffic
Web	SocialNetwork > MIXI > Image	17039398	mixi traffic
Web	SocialNetwork > MIXI > Text	17104934	mixi traffic
Web	SocialNetwork > MIXI > Video	17170470	mixi traffic

Table 2-1 Default applications (continued)

Application group	Sub-components	Value	Description
Web	SocialNetwork > MIXI > XWORLD	17236006	mixi traffic
Web	SocialNetwork > MYSPACE	16777251	MySpace traffic
Web	SocialNetwork > MYSPACE > Application	16908323	MySpace traffic
Web	SocialNetwork > MYSPACE > Audio	16973859	MySpace traffic
Web	SocialNetwork > MYSPACE > Database	16842787	MySpace traffic
Web	SocialNetwork > MYSPACE > Image	17039395	MySpace traffic
Web	SocialNetwork > MYSPACE > Text	17104931	MySpace traffic
Web	SocialNetwork > MYSPACE > Video	17170467	MySpace traffic
Web	SocialNetwork > MYSPACE > XWORLD	17236003	MySpace traffic
Web	SocialNetwork > NETLOG	16777252	Netlog traffic
Web	SocialNetwork > NETLOG > Application	16908324	Netlog traffic
Web	SocialNetwork > NETLOG > Audio	16973860	Netlog traffic
Web	SocialNetwork > NETLOG > Database	16842788	Netlog traffic
Web	SocialNetwork > NETLOG > Image	17039396	Netlog traffic
Web	SocialNetwork > NETLOG > Text	17104932	Netlog traffic
Web	SocialNetwork > NETLOG > Video	17170468	Netlog traffic
Web	SocialNetwork > NETLOG > XWORLD	17236004	Netlog traffic
Web	SocialNetwork > NING	16777261	Ning traffic
Web	SocialNetwork > NING > Application	16908333	Ning traffic
Web	SocialNetwork > NING > Audio	16973869	Ning traffic
Web	SocialNetwork > NING > Database	16842797	Ning traffic
Web	SocialNetwork > NING > Image	17039405	Ning traffic
Web	SocialNetwork > NING > Text	17104941	Ning traffic
Web	SocialNetwork > NING > Video	17170477	Ning traffic
Web	SocialNetwork > NING > XWORLD	17236013	Ning traffic
Web	SocialNetwork > PLAXO	16777253	Plaxo traffic
Web	SocialNetwork > PLAXO > Application	16908325	Plaxo traffic
Web	SocialNetwork > PLAXO > Audio	16973861	Plaxo traffic
Web	SocialNetwork > PLAXO > Database	16842789	Plaxo traffic
Web	SocialNetwork > PLAXO > Image	17039397	Plaxo traffic
Web	SocialNetwork > PLAXO > Text	17104933	Plaxo traffic
Web	SocialNetwork > PLAXO > Video	17170469	Plaxo traffic
Web	SocialNetwork > PLAXO > XWORLD	17236005	Plaxo traffic
Web	SocialNetwork > QQ	16777262	QQ traffic
Web	SocialNetwork > QQ > Application	16908334	QQ traffic

Table 2-1 Default applications (continued)

Application group	Sub-components	Value	Description
Web	SocialNetwork > QQ > Audio	16973870	QQ traffic
Web	SocialNetwork > QQ > Database	16842798	QQ traffic
Web	SocialNetwork > QQ > Image	17039406	QQ traffic
Web	SocialNetwork > QQ > Text	17104942	QQ traffic
Web	SocialNetwork > QQ > Video	17170478	QQ traffic
Web	SocialNetwork > QQ > XWORLD	17236014	QQ traffic
Web	SocialNetwork > RENREN	16777263	Renren traffic
Web	SocialNetwork > RENREN > Application	16908335	Renren traffic
Web	SocialNetwork > RENREN > Audio	16973871	Renren traffic
Web	SocialNetwork > RENREN > Database	16842799	Renren traffic
Web	SocialNetwork > RENREN > Image	17039407	Renren traffic
Web	SocialNetwork > RENREN > Text	17104943	Renren traffic
Web	SocialNetwork > RENREN > Video	17170479	Renren traffic
Web	SocialNetwork > RENREN > XWORLD	17236015	Renren traffic
Web	Squid	5070	Squid traffic
Web	Tex > ENRICHED	17131008	ENRICHED traffic
Web	Text	17104896	Web text traffic
Web	Text > CSS	17132800	CSS traffic
Web	Text > HTML	17131264	HTML traffic
Web	Text > PLAIN	17131520	PLAIN traffic
Web	Text > RICHTEXT	17131776	RICHTEXT traffic
Web	Text > TabSeparatedValue	17132288	TabSeparatedValue traffic
Web	Text > VNDRNRealText	17132544	VNDRNRealText traffic
Web	Text > XML	17133056	XML traffic
Web	Twitter	16777247	Twitter traffic
Web	Twitter > Application	16908319	Twitter traffic
Web	Twitter > Audio	16973855	Twitter traffic
Web	Twitter > Database	16842783	Twitter traffic
Web	Twitter > Image	17039391	Twitter traffic
Web	Twitter > Text	17104927	Twitter traffic
Web	Twitter > Video	17170463	Twitter traffic
Web	Twitter > XWORLD	17235999	Twitter traffic
Web	UncommonSocialWeb	16777270	Uncommon social web traffic
Web	UncommonSocialWeb > Application	16908342	Uncommon social web traffic
Web	UncommonSocialWeb > Audio	16973878	Uncommon social web traffic
Web	UncommonSocialWeb > Database	16842806	Uncommon social web traffic

Table 2-1 Default applications (continued)

Application group	Sub-components	Value	Description
Web	UncommonSocialWeb > Image	17039414	Uncommon social web traffic
Web	UncommonSocialWeb > Text	17104950	Uncommon social web traffic
Web	UncommonSocialWeb > Video	17170486	Uncommon social web traffic
Web	UncommonSocialWeb > XWORLD	17236022	Uncommon social web traffic
Web	Video	17170432	Web video traffic traffic
Web	Video > AVI	17198848	AVI traffic
Web	Video > MsVideo1	17199360	MsVideo1 traffic
Web	Video > MsVideo2	17199616	MsVideo2 traffic
Web	Video > QUICKTIME	17199872	QUICKTIME traffic
Web	Video > VNDRNRealVideo	17200128	VNDRNRealVideo traffic
Web	Video > VNDVivo	17200384	VNDVivo traffic
Web	Video > XLsASF	17200640	XLsASF traffic
Web	Video > XLsASX	17200896	XLsASX traffic
Web	Video > XMsASF	17201408	XMsASF traffic
Web	Video > XMsASX	17201664	XMsASX traffic
Web	Video > XMsVideo	17201920	XMsVideo traffic
Web	Video > XSgiMovie	17202176	XSgiMovie traffic
Web	Web	1010	Web traffic
Web	Web	1012	Web traffic
Web	Web	9999	Web traffic
Web	Web	1020	Web traffic
Web	Web-Port	21739	Web-Port traffic
Web	WebFileTransfer	5061	WebFileTransfer traffic
Web	WebFileTransfer	5000	WebFileTransfer traffic
Web	WebFileTransfer	5060	WebFileTransfer traffic
Web	WebFileTransfer	5062	WebFileTransfer traffic
Web	WebMediaAudio	5004	WebMediaAudio traffic
Web	WebMediaAudio	5021	WebMediaAudio traffic
Web	WebMediaAudio	5003	WebMediaAudio traffic
Web	WebMediaAudio	5001	WebMediaAudio traffic
Web	WebMediaAudio	5031	WebMediaAudio traffic
Web	WebMediaDocuments	5010	WebMediaDocuments traffic
Web	WebMediaDocuments	5012	WebMediaDocuments traffic
Web	WebMediaDocuments	5014	WebMediaDocuments traffic
Web	WebMediaDocuments	5040	WebMediaDocuments traffic
Web	WebMediaDocuments	5011	WebMediaDocuments traffic

Table 2-1 Default applications (continued)

Application group	Sub-components	Value	Description
Web	WebMediaDocuments	5030	WebMediaDocuments traffic
Web	WebMediaDocuments	5013	WebMediaDocuments traffic
Web	WebMediaVideo	5020	WebMediaAudio traffic
Web	WebMediaVideo	5007	WebMediaDocuments traffic
Web	WebMediaVideo	5002	WebMediaVideo traffic
Web	WebMediaVideo	5008	WebMediaVideo traffic
Web	Webmin	51350	Webmin traffic
Web	XWORLD	17235968	XWORLD traffic
Web	XWORLD > XVrml	72679681	XWORLD > XVrml traffic
Web	Yahoo	16777265	Yahoo traffic
Web	Yahoo > Application	16908337	Yahoo traffic
Web	Yahoo > Audio	16973873	Yahoo traffic
Web	Yahoo > Database	16842801	Yahoo traffic
Web	Yahoo > Image	17039409	Yahoo traffic
Web	Yahoo > Text	17104945	Yahoo traffic
Web	Yahoo > Video	17170481	Yahoo traffic
Web	Yahoo > XWORLD	17236017	Yahoo traffic
Web	Youtube	16777266	YouTube traffic
Web	Youtube > Application	16908338	YouTube traffic
Web	Youtube > Audio	16973874	YouTube traffic
Web	Youtube > Database	16842802	YouTube traffic
Web	Youtube > Image	17039410	YouTube traffic
Web	Youtube > Text	17104946	YouTube traffic
Web	Youtube > Video	17170482	YouTube traffic
Web	Youtube > XWORLD	17236018	YouTube traffic

3 ICMP TYPE AND CODE IDS

This reference provides information about default ICMP type and Code IDs.

Identifying default ICMP types

The following table lists the default ICMP Codes:

Table 3-1 ICMP types

ICMP Type	Description
0	**EchoReply**
3	DestinationUnreachable
4	SourceQuench
5	Redirect
8	Echo
9	RouterAdvertisement
10	RouterSelection
11	TimeExceeded
12	ParameterProblem
13	Timestamp
14	TimestampReply
15	InformationRequest
16	InformationReply
17	AddressMaskRequest
18	AddressMaskReply
30	Traceroute

Identifying default ICMP codes

The following table lists the default ICMP codes:

Table 3-2 ICMP codes

ICMP Code		Description
3	**Destination Unreachable Codes**	
	0	Net Unreachable
	1	Host Unreachable
	2	Protocol Unreachable
	3	Port Unreachable
	4	Fragmentation Needed and Don't Fragment was Set
	5	Source Route Failed
	6	Destination Network Unknown
	7	Destination Host Unknown
3	**Destination Unreachable Codes**	
	8	Source Host Isolated
	9	Communication with Destination Network is Administratively Prohibited
	10	Communication with Destination host is Administratively Prohibited
	11	Destination Network Unreachable for Type of Service
	12	Destination Host Unreachable for Type of Service
	13	Communication Administratively Prohibited
	14	Host Precedence Violation
	15	Precedence cutoff in effect
5	**Redirect Codes**	
	0	Redirect Datagram for the Network (or subnet)
	1	Redirect Datagram for the Host
	2	Redirect Datagram for the Type of Service and Network
	3	Redirect Datagram for the Type of Service and Host
11	**Time Exceeded Codes**	
	0	Time to Live exceeded in Transit
	1	Fragment Reassembly Time Exceeded
12	**Parameter Problem Codes**	
	0	Pointer indicates the error

Table 3-2 ICMP codes (continued)

ICMP Code	Description
1	Missing a Required Option
2	Bad Length

4 PORT IDS

This reference provides information about default port IDs used by QRadar.

The following table lists the default common ports:

Table 4-1 Port IDs

Port	Protocol	Protocol description
20	FTP	File Transfer Protocol
21	FTP	File Transfer Protocol
22	SSH	Secure Shell
23	Telnet	
25	SMTP	Send Mail Transfer Protocol
53	DNS	Domain Name Service
80	HTTP	HyperText Transfer Protocol
81	HTTP	HyperText Transfer Protocol
110	POP3	Post Office Protocol - version 3
119	NNTP News	Network New Transfer Protocol
123	NTP	Network Time Protocol
137	NetBIOS	Network Basic Input/Output System
143	IMAP	Internet Message Access Protocol
161	SNMP	Simple Network Management Protocol
162 - 164	SNMP trap	Simple Network Management Protocol trap
389	LDAP	Lightweight Directory Access Protocol
391	NSRMP	Network Security Risk Management Protocol
392	NSRMP	Network Security Risk Management Protocol
443	SecureWeb	
500	IPSec	Internet Protocol Security
636	LDAP	Lightweight Directory Access Protocol
2005	Oracle	

Table 4-1 Port IDs (continued)

Port	Protocol	Protocol description
2049	NFS	Network File System
4500	IPSec	Internet Protocol Security
5432	PostgreSQL	
8080	HTTP	

5 PROTOCOL IDS

This referecne provides information about default protocols IDs used in QRadar.

The following table lists the default common protocols:

Table 5-1 Protocol IDs

Protocol ID	Protocol port description
6	TCP
17	UDP
1	ICMP
2	IGMP
38	IDPR-CMTP
40	IPv6
46	RSVP
47	GRE
50	ESP
51	AH
54	NARP
89	OSPFIGP
94	IPIP
99	ANY
132	SCTP

A NOTICES AND TRADEMARKS

What's in this appendix:

This section describes some important notices, trademarks, and compliance information.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the

capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at *http://www.ibm.com/legal/copytrade.shtml*.

The following terms are trademarks or registered trademarks of other companies:

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.