Release Notes for NBAR2 Protocol Pack 19.0.0

Overview

NBAR2 Protocol Pack 19.0.0 provides classification improvements and bug fixes.

- SIP code refactoring and performance improvement to allow more bundles in a burst.
- Fixed a DNS socket cache issue to resolve DNS customization issue CSCuz39567.

Supported Platforms

NBAR2 Protocol Pack 19.0.0 is supported on the following platforms:

- Cisco ASR 1000 Series Routers
- Cisco ISR 4400 Series Routers
- Cisco ISR Generation 2 Routers

Supported Releases

NBAR Protocol Pack 19.0.0 is supported on the following releases:

Built-in	Supported on Maintenance Releases
-	Cisco IOS XE 3.16.2S Version 15.5(3)S2 and later maintenance releases of 3.16.(x)S/15.5(3)S(x)
	Cisco IOS Version 15.5(3)M2 and later and later maintenance releases of 15.5(3)M(x)

New Protocols in NBAR2 Protocol Pack 19.0.0

No new protocols in NBAR2 Protocol Pack 19.0.0.

Updated Protocols in NBAR2 Protocol Pack 19.0.0

The table below lists the protocol(s) updated in NBAR2 Protocol Pack 19.0.0.

Protocol	Updates
dns	Updated signatures

Deprecated Protocols in NBAR2 Protocol Pack 19.0.0

In this release, no protocols have changed status to deprecated.

Caveats in NBAR2 Protocol Pack 19.0.0

Note If you have an account on Cisco.com, you can view information on select caveats, using the Bug Search Tool (https://tools.cisco.com/bugsearch/search).

Resolved Caveats in NBAR2 Protocol Pack 19.0.0

The following table lists the caveats resolved in NBAR2 Protocol Pack 19.0.0:

Resolved Caveat	Description
CSCuz39567	DNS customization does not work under some conditions

Known Caveats in NBAR2 Protocol Pack 19.0.0

The following table lists the known caveats in NBAR2 Protocol Pack 19.0.0:

Known Caveat	Description
CSCuh49380	PCoIP session-priority configuration limitation.
CSCuh53623	Segmented packets are not classified when using NBAR sub classification.
CSCun61772	IPv4 bundles might be used in IPv6 traffic.

Downloading NBAR2 Protocol Pack 19.0.0

NBAR2 Protocol Packs are available for download on the Cisco.com software download page (http://www.cisco.com/cisco/software/navigator.html). On the download page, specify a platform model to display software available for download. One software option will be **NBAR2 Protocol Packs**.

Example

To display protocol packs available for the Cisco ASR 1001 platform, the navigation path is:

Products > Routers > Service Provider Edge Routers > ASR 1000 Series Aggregation Services Routers > ASR 1001 Router

Special Notes and Limitations

Protocol Name	Special Note or Limitation
apple-app-store	Login and a few encrypted sessions are classified as iTunes.
bittorrent	HTTP traffic generated by the bitcomet bittorrent client might be classified as HTTP.
capwap-data	For capwap-data to be classified correctly, capwap-control must also be enabled.
ftp	During configuring QoS class-map with ftp-data, the FTP protocol must be selected. As an alternative, the FTP application group can be selected.
hulu	Encrypted video streaming generated by hulu may be classified as its underlying protocol rtmpe.
logmein	Traffic generated by the logmein android app may be classified incorrectly as ssl.

Protocol Name	Special Note or Limitation
ms-lync	Login and chat traffic generated by the ms-lync client may be classified incorrectly as ssl.
pcanywhere	Traffic generated by pcanywhere for mac may be classified as unknown.
perfect-dark	Some perfect-dark sessions may be classified as unknown.
qq-accounts	Login to QQ applications which is not via the internet may not be classified as qq-accounts.
secondlife	Voice traffic generated by secondlife may be classified incorrectly as ssl.
ssl	The Sub Classification (SC) mechanism was modified to include search for wildcard. **Note** The SC rule for the part of the Server Name Indication (SNI) or the common name (CN) can now include a wildcard. If a wildcard is not used, the complete SNI or the CN is required. For example, you can either use, "*.pqr.com" or "abc.pqr.com" to classify abc.pqr.com.

Additional References

Related Documentation

Related Topic	Document Title
Application Visibility and Control	Cisco Application Visibility and Control User Guide
Classifying Network Traffic Using NBAR	Classifying Network Traffic Using NBAR module
NBAR Protocol Pack	NBAR Protocol Pack module
QoS: NBAR Configuration Guide	QoS: NBAR Configuration Guide
QoS Command Reference	Quality of Service Solutions Command Reference