Juniper Networks | Engineering Simplicity

Juniper Secure Analytics Network Insights User Guide

Published
2023-07-25

RELEASE
7.5.0

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Secure Analytics Network Insights User Guide
7.5.0

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About This Guide | v

1 Introduction to Installing Network Insights

Introduction to Installing Network Insights | 2

2 Network Insights Overview

Network Insights Overview | 4

What's New for Users in Network Insights 7.5.0 | 5

3 Network Insights Use Cases

Network Insights Use Cases | 8

4 Flow Inspection Levels

Flow Inspection Levels | 12

- Basic Inspection | 14
- Enriched Inspection | 16
- Advanced Inspection | 26
- Suspicious Content in Network Flows | 27

5 Network Flow Data

Network Flow Data | 30

- Including Network Insights Data in Searches | 31
- Identifying the Source of the Flow Data | 33
- Parsing DNS Query and Response Fields | 34
- Content Extensions | 36

6 X-Force Integration

X-Force Integration in Network Insights | 38

- Suspect Content Descriptions Derived from X-Force | 38
- Flow property integration with X-Force Exchange | 40

Direct Lookups for IP Reputation Classifications | **40**

7 **Supported Inspectors**

Supported Inspectors | 43

Protocol Inspectors | **43**

Document Formats | **44**

Application Detection | **45**

About This Guide

Use this guide to analyze network data in real-time by using JSA Network Insights.

1
CHAPTER

Introduction to Installing Network Insights

Introduction to Installing Network Insights

IN THIS SECTION

- Intended Audience | 2
- Technical Documentation | 2
- Contacting Customer Support | 2

This guide contains information about analyzing network data in real-time by using Network Insights.

Intended Audience

Investigators extract information from the network traffic and focus on security incidents, and threat indicators.

Technical Documentation

To find JSA product documentation on the web, including all translated documentation, access the JSA Series Virtual Appliance Documentation.

Contacting Customer Support

For information, contact Juniper Customer Support.

2
CHAPTER

Network Insights Overview

Network Insights Overview | 4

What's New for Users in Network Insights 7.5.0 | 5

Network Insights Overview

SUMMARY

Network Insights provides in-depth visibility into network communications on a real-time basis to extend the capabilities of your JSA deployment.

IN THIS SECTION

- Benefits of Network Insights | 4

Through the deep analysis of network activity and application content, Network Insights empowers Juniper Secure Analytics to detect threat activity that would otherwise go unnoticed.

Network Insights provides in-depth analysis of both network metadata and application content to detect suspicious activity that is hidden among normal traffic and extract content to provide JSA with visibility into network threat activity. The intelligence that is provided by Network Insights integrates seamlessly with traditional data sources and threat intelligence to extend JSA detection, analysis, and threat detection capabilities.

Network Insights provides visibility across a range of use cases, including:

- Malware detection and analysis
- Phishing email and campaign detection
- Insider threats
- Lateral movement attack detection
- Data exfiltration protection
- Identify compliance gaps

Benefits of Network Insights

The following list highlights some of the benefits of using Network Insights:

- Uses in-depth packet inspection to identify advanced threats and malicious content.
- Extends the capabilities of JSA to detect phishing attacks, malware intrusions, lateral movement, and data exfiltration.
- Records application activities, captures key artifacts, and identifies assets, applications, and users that participate in network communications.

- Applies Layer 7 content analysis for advanced security insights.
- File analytics analyzes and enables tracking of files.

What's New for Users in Network Insights 7.5.0

IN THIS SECTION

- Modified process for identifying file types | 5
- More integration with IBM X-Force | 5
- Improved application detection | 6

JSA Network Insights 7.5.0 provides users with more IBM X-Force Exchange integration and improvements to file type identification and application detection.

Modified process for identifying file types

Earlier versions of Network Insights used the Apache Tiki library to identify the file type, but only at the advanced inspection level.

JSA Network Insights 7.5.0 Update Pack 1 uses a different library to identify file types, and does the identification at all inspection levels as part of the main traffic inspection process.

With this change, fewer files are sent to the Apache Tika library for analysis, which might result in improved performance at the advanced inspection level. Individual performance improvements depend on the volume and type of files that are sent for analysis.

More integration with IBM X-Force

JSA Network Insights 7.5.0 introduces a new series of suspect content descriptions that are derived from IBM X-Force signatures. When a flow matches one or more of the X-Force signatures, the suspect content description is shown on the **Network Activity** tab.

Also introduced in this release, some properties on the **Flow information** window are directly integrated with IBM X-Force Exchange. With a single click, you can quickly determine whether the property value requires further investigation.

Improved application detection

JSA Network Insights 7.5.0 includes protocol parsing improvements and can now analyze the payload to identify 300 more applications.

After the upgrade is complete, view these files to see the complete list of applications that can be identified:

- **/opt/ibm/xforce/metadata/protocols.hdr** (column headers)
- **/opt/ibm/xforce/metadata/protocols.csv** (values)

3

CHAPTER

Network Insights Use Cases

Network Insights Use Cases | 8

Network Insights Use Cases

SUMMARY

Network Insights provides in-depth visibility into network communications and application content to empower Juniper Secure Analytics to detect threat activity. You can use Network Insights to detect and analyze malware, phishing, insider threats, lateral movement attacks, data exfiltration, and compliance gaps.

IN THIS SECTION

- Malware Detection and Analysis | 8
- Phishing Email and Campaign Detection | 8
- Insider Threats | 9
- Lateral Movement Attack Detection | 9
- Data Exfiltration Protection | 9
- Identify Compliance Gaps | 10

Malware Detection and Analysis

Malware frequently morphs to avoid detection. You can use Network Insights to detect malware based on file hashes and file activity, and observe and analyze artifacts such as:

- Names
- Properties
- Movement
- Suspicious content

Phishing Email and Campaign Detection

Phishing can hide in plain sight by disguising its activity within the volumes of normal emails. You can prepare for and react to malicious emails by using Network Insights to analyze:

- Sources
- Targets
- Subject

- Content

Insider Threats

You can integrate Network Insights with the User Behavior Analytics app to improve threat detection. Use the Network Insights analytics to recognize:

- High-risk users
- Potential targets of phishing
- Negative sentiment
- Suspicious behaviors

Lateral Movement Attack Detection

Network Insights can trace anomalous communications:

- Reconnaissance
- Data transfers
- Rogue and malicious actors

Data Exfiltration Protection

Data can be exfiltrated through many methods. Use Network Insights to identify and track suspicious files such as:

- DNS abnormalities
- Sensitive content
- Aberrant connections
- Aliases

Identify Compliance Gaps

Network Insights allows for continuous monitoring of enterprise, industry, and regulatory compliance.

4

CHAPTER

Flow Inspection Levels

Flow Inspection Levels | 12

Flow Inspection Levels

IN THIS SECTION

- Basic Inspection | 14
- Enriched Inspection | 16
- Advanced Inspection | 26
- Suspicious Content in Network Flows | 27

The flow inspection level determines how much data is analyzed and extracted from the network flows. By default, the flow inspection level is a global setting that is configured in the **System Settings** on the **Admin** tab. It applies to all appliances in your deployment. You can override the global setting by configuring a custom flow inspection level for each appliance.

In a stacked configuration, each stack can have a different inspection level, but all appliances within a stack must have the same inspection level.

Basic Inspection Level

The **Basic** level is the lowest level of flow inspection. This level supports the highest bandwidth, but generates the least amount of flow information.

The attributes that Network Insights captures using the basic flow inspection level are similar to what you get out of a router or network switch that does not perform deep packet inspection, and include the following types of information:

- Source and destination information
- Network protocol
- Application ID
- Byte and packet counters
- Time of first and last packets
- Quality of service

- VLAN tags

At the **Basic** inspection level, Network Insights creates a data flow that captures information about the network communication. The data flow includes payload samples, and shows the byte and packet size counters. The **Basic** inspection level collects the same information as the QFlow process.

Enriched Inspection Level

With the enriched inspection level, each flow is identified and inspected by one of the protocol or domain inspectors, and many kinds of attributes can be generated from that inspection.

The **Enriched** inspection level provides the following types of information:

- Usernames, email addresses, chat IDs
- Search arguments
- Host information
- HTTP, FTP, SMTP, SSL and TLS fields
- DNS queries and responses
- File name, type, size, hash, and entropy
- Last proxy, XFF, True Client IP
- Suspect content
- Web categories
- Configurable content-based suspect content (YARA rules)

At the **Enriched** and **Advanced** inspection levels, Network Insights creates both data flows and content flows. The content flow shows what was found inside the data flow with the deeper level of inspection. Content flows do not include payload samples, and all byte and packet counters appear as zero. They are linked to the data flow by the **Flow ID** field.

You can identify content flows in the following ways:

- In the **Flow Information** window, the **Flow Type** field shows **Standard Flow (Content Flow)**.
- On the **Network Activity** tab, the tooltip for the **Flow Type** icon shows **Standard Flow (Content Flow)**.

Advanced Inspection Level

Advanced inspection is the highest level of inspection, and it is the default setting for new installations. Through comprehensive analysis of the application content, it builds on the flow attributes that are extracted at the Enriched inspection level.

The **Advanced** inspection level provides the following types of information:

- Content extraction
- Personal information detection
- Confidential data detection
- Embedded scripts
- Redirects
- Extra file metadata

The advanced inspection level also performs content analysis, which can yield more suspect content values than the Enriched level. For example, when set to the **Advanced** inspection level, Network Insights looks deep within files to identify suspect content such as embedded scripts in PDF or Microsoft documents.

Similar to the enriched level, a content flow is created to show what Network Insights found while doing the deeper level of inspection of the data flow.

Basic Inspection

SUMMARY

The **Basic** inspection level supports high bandwidth but generates the least amount of flow information. The **Basic** level inspection creates standard flow records known as data flows.

NOTE: The data must exist in the source content so that the field is populated in JSA. For example, some content is populated by the X-Force Threat Intelligence feed, but the field may appear empty in JSA if the information is not available in X-Force.

The following table shows the fields that are populated when Network Insights is configured to use the **Basic** inspection level.

Table 1: Content that is Populated with the Basic Inspection Level

Query builder name	Advanced search name	Data source
Application	`applicationid`	Multiple sources, such as Inspectors and X-Force. The attribute is populated by default.
Customer VLAN ID	`"customer vlan id"`	Populated only when the flow source or destination address came from 802.1q VLAN header data.
Destination DSCP	`destinationdscp`	IP quality of service derived from the IPv4 or IPv6 header of the flow packet.
Destination Flags	`destinationflags`	TCP header of the flow packet.
Destination IP address	`destinationip`	IPv4 or IPv6 header of the flow packet.
Destination Port	`destinationport`	TCP or UDP header of the flow packet.
Enterprise VLAN ID	`"enterprise vlan id"`	Populated only when the flow source or destination address came from 802.1q VLAN header data.
First Packet Time	`firstpackettime`	Assigned by Network Insights.
Flow ID	`flowid`	Assigned by Network Insights.
IP protocol	`protocolid`	IPv4 or IPv6 header of the flow.
Last Packet Time	`lastpackettime`	Assigned by Network Insights.

Table 1: Content that is Populated with the Basic Inspection Level *(Continued)*

Query builder name	Advanced search name	Data source
Source DSCP	`sourcedscp`	IP quality of service derived from the IPv4 or IPv6 header of the flow packet.
Source Flags	`sourceflags`	TCP header of the flow packet.
Source IP address	`sourceip`	IPv4 or IPv6 header of the flow packet.
Source port	`sourceport`	TCP or UDP header of the flow packet.
Total bytes per packet	`sourcebytes`, `destinationbytes`	Assigned and maintained by Network Insights*.
Total Packets	`sourcepackets`, `destinationpackets`	Assigned and maintained by Network Insights*.
VLAN Tag	`"vlan tag"`	Populated only when the flow source or destination address came from 802.1q VLAN header data.
VXLAN Network Identifier	`"vxlan network indentifier"`	Populated only when the flow contains VXLAN header data.

Enriched Inspection

SUMMARY

At the **Enriched** inspection level, each flow is identified and inspected by a protocol or domain inspector. When the flow inspection level is set to **Enriched**, Network Insights creates content flows.

NOTE: The data must exist in the source content so that the field is populated in JSA. For example, some content is populated by the X-Force Threat Intelligence feed, but the field might appear empty in JSA if the information is not available in X-Force.

The following table shows the fields that are populated when Network Insights is configured to use the **Enriched** inspection level.

Table 2: Content that is populated with the Enriched inspection level

Query Builder name	Advanced Search name	Description
Action	`action`	Populated when the flow analysis indicates an action on an HTTP flow. Possible values for the action are: • Write/Post/Chat • Stream/Download • Share • Start App • Audio Chat/Video Chat • Software/AV Updates The flow analysis is based on X-Force data, and the field is populated only when the X-Force data is available.
Authentication mechanism	`"authentication mechanism"`	The means by which the client was authenticated.
Content subject	`"content subject"`	If populated, extracted from the `Subject` field of the flow content. For example, the subject might come from an email or it might be embedded in the metadata.
Content Type	`"content type"`	HTTP, Content Inspector Populated only when the file type is not recognized.

Table 2: Content that is populated with the Enriched inspection level *(Continued)*

Query Builder name	Advanced Search name	Description
DNS Query ID	`"dns query id"`	Populated only if the flow contains information about a DNS request or response.
DNS Domain Name	`"dns domain name"`	Populated only if the flow contains information about a DNS request.
DNS Request Type	`"dns request type"`	Populated only if the flow contains information about a DNS request.
DNS Response Code	`"dns response code"`	Populated only if the flow contains information about a DNS response.
DNS Flags	`"dns flags"`	Populated only if the flow contains information about a DNS request.
DNS Answers	`"dns answers"`	All DNS fields (formatted list). Populated only if the flow contains information about a DNS response.
DNS Raw Answer	`"dns raw answer"`	All DNS fields (binary format). Populated only if the flow contains information about a DNS response.
File Entropy	`"file entropy"`	Populated only when a complete file is found embedded in the flow data.
File Name	`"file name"`	Populated only when a named file is found embedded in the flow data.
File Size	`"file size"`	Populated only when a complete file is found embedded in the flow data.
FTP Command	`"ftp command"`	FTP command that was used.
FTP ReplyCode	`"ftp reply code"`	Numerical code that is issued by the FTP server in response to the FTP command.

Table 2: Content that is populated with the Enriched inspection level *(Continued)*

Query Builder name	Advanced Search name	Description
FTP Response	`"ftp response"`	Description for the numerical reply code that is issued by the FTP server.
HTTP Host	`"http host"`	Host field in the HTTP request. Populated only if HTTP protocol is used.
HTTP Method	`"http method"`	Method in the HTTP request, indicating the preferred action to be performed. Populated only if the HTTP protocol is used.
HTTP Referrer	`"http referrer"`	Referrer field in the HTTP request. Populated only if HTTP protocol is used.
HTTP Response Code	`"http response code"`	Response from the HTTP request. Populated only if HTTP protocol is used.
HTTP Server	`"http server"`	Server field in the HTTP request. Populated only if HTTP protocol is used.
HTTP User Agent	`"http user agent"`	User Agent field in the HTTP request. Populated only if HTTP protocol is used.
HTTP Version	`"http version"`	Version field in the HTTP request. Populated only if HTTP protocol is used.
Kerberos Cipher Suite	`"kerberos cipher suite"`	The suite of ciphers that is used to encrypt the Kerberos ticket.
Kerberos Client Principal Name	`"kerberos client principal name"`	The identity that the ticket is being issued to. For example, the user or device that is seeking a ticket to authenticate themselves to a service.
Kerberos Issued Ticket Hash	`"kerberos issued ticket hash"`	A hash of the Kerberos ticket that was issued to the client.

Table 2: Content that is populated with the Enriched inspection level *(Continued)*

Query Builder name	Advanced Search name	Description
Kerberos Presented Ticket Hash	`"kerberos presented ticket hash"`	A hash of the Kerberos ticket that was presented to gain access to a resource. This property is populated by the Kerberos inspector, as well as the HTTP and SMB inspectors when applicable.
Kerberos Realm	`"kerberos realm"`	The Kerberos realm in which this activity takes place.
Kerberos Server Principal Name	`"kerberos server principal name"`	The identity of the service that the ticket is being issued for. For example, the service that the user wants to access.
Last Proxy Basis	`"last proxy basis"`	Where an HTTP request was found to be explicitly forwarded, the type of HTTP header that directed the forwarding. The **Last Proxy Basis** attribute might include one of the following values: • RFC 7239 forwarding header • X-Forwarded-For header • Akamai True-Client-IP header
Last Proxy IPv4	`"last proxy ipv4"`	The final forwarded destination, which is shown as an IPv4 address. Populated only if HTTP protocol is used and forwarding was detected.
Last Proxy IPv6	`"last proxy ipv6"`	The final forwarded destination, which is shown as an IPv6 address. Populated only if HTTP protocol is used and forwarding was detected.
MD5 File Hash	`"md5 file hash"`	Populated with the MD5 hash of the original file when a file is extracted from the flow data.

Table 2: Content that is populated with the Enriched inspection level *(Continued)*

Query Builder name	Advanced Search name	Description
Originating User	`"originating user"`	Populated from multiple sources when the origin user can be detected, such as flow data for email or chat messages.
Password	`password`	Populated only when a cleartext password exchange is detected in the flow. For example, a cleartext password exchange in an FTP flow.
Protocol Name	`"protocol name"`	Populated on all flows that are processed by an inspector.
Protocol Version	`"protocol version"`	Populated only when the version is extracted by the inspector. Protocol version extraction is supported by the following inspectors: • NFS Version 3 • POP Version 3 • SSL Version 3 • TLS (all versions) • HTTP (all versions) • ICAP (all versions) • SMB (all versions, plus dialect where applicable) • SSH (all versions) • RDP (all versions)
RDP Encryption Method	`"rdp encryption method"`	Populated with the encryption method when the flow is associated with Remote Desktop Protocol (RDP).
RDP Encryption Level	`"rdp encryption level"`	Populated with the encryption level when the flow is associated with Remote Desktop Protocol (RDP).
Recipient Users	`"recipient users"`	Populated if one or more destination users are detected in the flow.

Table 2: Content that is populated with the Enriched inspection level *(Continued)*

Query Builder name	Advanced Search name	Description
Request URL	`"request url"`	Populated only when a URL string is detected in HTTP flow data.
Search Arguments	`"search arguments"`	Populated only when the pattern of a search request is detected in HTTP flow data.
SHA1 File Hash	`"sha1 file hash"`	Populated with the SHA1 hash of the original file when a file is extracted from the flow data.
SHA256 File Hash	`"sha256 file hash"`	Populated with the SHA256 hash of the original file when a file is extracted from the flow data.
SMTP Hello	`"smtp hello"`	Populated for flows that initiate an SMTP request. Captures the data that follows the `HELO` command. For more information, see Request for Comments (RFC) 2821 and 1651.
SSL/TLS Cipher Suite	`"ssl/tls cipher suite"`	The cipher suite specification that is agreed upon by the client and server to use for the session.
SSL/TLS Compression Method	`"ssl/tls compression method"`	The compression method that is agreed upon by the client and server to use for the session. The method is typically null, as most clients do not support TLS compression due to the susceptibility to protocol level attacks.
SSL/TLS Session ID	`"ssl/tls session id"`	The session identifier.
SSL/TLS Version	`"ssl/tls version"`	The version of SSL or TLS. The following versions are detected: • SSLv3 • TLSv1.0 • TLSv1.1 • TLSv1.2

Table 2: Content that is populated with the Enriched inspection level *(Continued)*

Query Builder name	Advanced Search name	Description
Suspect Content Descriptions	`"suspect content descriptions"`	Populated from multiple sources when a suspicious entity is detected. For example, the suspect content might come from the website category, embedded links, or Yara rules.
TFTP Status	`"tftp status"`	TFTP read or write request. Populated only if the transfer protocol is TFTP.
TFTP Mode	`"tftp mode"`	The mode of the TFTP file transfer. Possible values are `netascii` or `octet`. Populated only when the transfer protocol is TFTP.
TFTP Requested Options	`"tftp requested options"`	The TFTP file transfer options that are negotiated before the transfer, which includes the following options: • `blocksize` allows the client and server to negotiate a block size for the file transfer. • `timeout` allows the client and server to set the timeout interval for the file that is transmitted. • `tsize` allows the side that receives the file to determine the size of the transfer. Populated only when the transfer protocol is TFTP.
TLS Application Layer Protocol	`"tls application layer protocol"`	The value of the application layer protocol that is agreed upon by the client and server, through the Application Layer Protocol Negotiation TLS extension.
TLS JA3 Hash	`"tls ja3 hash"`	Populated with the JA3 hash of the original file that is sent by the client.
TLS JA3S Hash	`"tls ja3s hash"`	Populated with the JA3S hash of the original file that is returned by the server.

Table 2: Content that is populated with the Enriched inspection level *(Continued)*

Query Builder name	Advanced Search name	Description
TLS Server Name Indication	`"tls server name indication"`	The value of the TLS Server Name Indication (SNI) extension. The client sends the SNI extension at the start of the handshake process to identify the server that they want to communicate with.
Web Categories	`"web categories"`	Populated only when the HTTP URL or endpoint matches a known X-Force web category.
X509 Certificate Extensions	`"x509 certificate extensions"`	Shows additional information about how the certificate can be used, identified, and verified. The X509 certificate extensions are shown as a comma-separated list.
X509 Certificate Fingerprint Hash	`"x509 certificate fingerprint hash"`	A hash of various fields in the certificate that can be used to fingerprint the certificate. This value can be useful in threat hunting and anomaly detection scenarios. For example, if valid certificates for the same subject with different fingerprint hashes are seen concurrently on different flows, then it might indicate that a man-in-the-middle attack is occurring on one set of flows.
X509 Certificate Issuer Common Name	`"x509 certificate issuer common name"`	The common name of the entity that issued the certificate. This field is the last 'CN = ' segment of the Issuer Name. For example, the value might look similar to this string: `GeoTrust RSA CA 2018`.
X509 Certificate Issuer Name	`"x509 certificate issuer name"`	The full name of the entity that issued the certificate. For example, the issuer name might look similar to this string: `C=US, O=DigiCert Inc, OU=www.digicert.com, CN=GeoTrust RSA CA 2018`.

Table 2: Content that is populated with the Enriched inspection level *(Continued)*

Query Builder name	Advanced Search name	Description
X509 Certificate Not-After Validity Timestamp	`"x509 certificate not-after validity timestamp"`	The timestamp of the last time that the certificate was valid. The value is the number of seconds since the epoch (1970-01-01 00:00:00 UTC). This value might be useful in understanding why the `Certificate invalid` suspicious content alert was generated.
X509 Certificate Not-Before Validity Timestamp	`"x509 certificate not-before validity timestamp"`	The timestamp of the earliest time at which the certificate is valid. The value is the number of seconds since the epoch (1970-01-01 00:00:00 UTC). This value might be useful in understanding why the `Certificate invalid` suspicious content alert was generated.
X509 Certificate Public Key Algorithm	`"x509 certificate public key algorithm"`	Identifies the algorithm that is used for the public key in the certificate; For example, `rsaEncryption`.
X509 Certificate Public Key Size	`"x509 certificate public key size"`	The size of the public key in the certificate. For example, the size of the key might be 2048 bits. This value can be useful in understanding why a `Weak public key length` suspicious content alert was generated.
X509 Certificate Serial Number	`"x509 certificate serial number"`	The serial number of the certificate. This is a number that uniquely identifies the certificate at the certificate authority. This value might be useful when cross referencing against a certificate revocation list.
X509 Certificate Signature Algorithm	`"x509 certificate signature algorithm"`	Identifies the algorithm that was used to sign the certificate. For example, the algorithm might be `sha256WithRSAEncryption`. If this value doesn't match the `To-Be-Signed Signature Algorithm`, then a `Signature Algorithm does not match To-Be-Signed Signature Algorithm` suspicious content alert is generated.

Table 2: Content that is populated with the Enriched inspection level *(Continued)*

Query Builder name	Advanced Search name	Description
X509 Certificate Subject Alternative Names	`"x509 certificate subject alternative names"`	Names that the certificate can also be used for. The names are displayed as a comma-separated list; For example, `www.ibm.com, ibm.com, 1.dam.s81c.com, 1.wwwstage.s81c.com, www-01.ibm.com, www-112.ibm.com`.
X509 Certificate Subject Common Name	`"x509 certificate subject common name"`	The common name of the entity that the certificate belongs to. This entry is the last 'CN = ' segment of the Subject Name; for example, `www.ibm.com`.
X509 Certificate Subject Name	`"x509 certificate subject name"`	The full name of the entity that the certificate belongs to; For example, `C=US, ST=New York, L=Armonk, O=IBM, CN=www.ibm.com`. The **Subject Name**, **Subject Common Name**, and **Subject Alternative Names** fields are useful in providing context about a flow that would otherwise appear as SSL/TLS.
X509 Certificate To-Be-Signed Signature Algorithm	`"x509 certificate to-be-signed signature algorithm"`	Identifies the algorithm that might have been used to sign the certificate. If this value doesn't match the **Signature Algorithm**, then a `Signature Algorithm does not match To-Be-Signed Signature Algorithm` suspicious content alert is generated.
X509 Certificate Version	`"x509 certificate version"`	The version of the X509 protocol that the certificate conforms to. For most certificates, this value is 3.

Advanced Inspection

SUMMARY

Through comprehensive analysis of the application content, the **Advanced** inspection level adds additional information to the flow attributes that are extracted at the **Enriched** inspection level.

Additional suspect content can also be detected through the content analysis that occurs at **Advanced** inspection level. For example, when set to the **Advanced** inspection level, Network Insights looks deep within files to identify suspect content such as embedded scripts in PDF or Microsoft documents.

Suspicious Content in Network Flows

SUMMARY

Network Insights checks for suspicious content in network flows at the enriched and advanced inspection levels.

The **Suspect Content Descriptions** field is populated by multiple data sources, such as website categories, embedded links, and Yara rules, and contains data only when a suspicious entity is detected.

The following list shows examples of the types of suspicious content that are detected at the enriched and advanced inspection levels:

Enriched inspection

- Identified protocol that runs on a non-standard port.
- SSL/TLS certificate that is used outside of its valid dates.
- Use of a self-signed certificate in SSL/TLS.
- Use of a weak public key length in SSL/TLS.
- Suspicious content via scanning with user provided Yara rules.
- Category of a website is one of several suspicious entries.

Advanced inspection

- Suspicious content in the transferred information.
- Excessive numbers of items that were discovered through regular expression matching.

- Credit card numbers, social security numbers, IP addresses, and email addresses.
- User-defined items that are discovered through regex matching that is marked as suspicious.
- Scripts in Office or PDF files.
- Embedded links in PDF files.
- Certificate has a non-DNS subject alternative name.
- Signature algorithm does not match the to-be-signed signature algorithm.
- BitTorrent handshake verification failure.
- X-Force signatures.

  For more information, see "Suspect content descriptions derived from X-Force" on page 38.

5
CHAPTER

Network Flow Data

Network Flow Data | 30

Network Flow Data

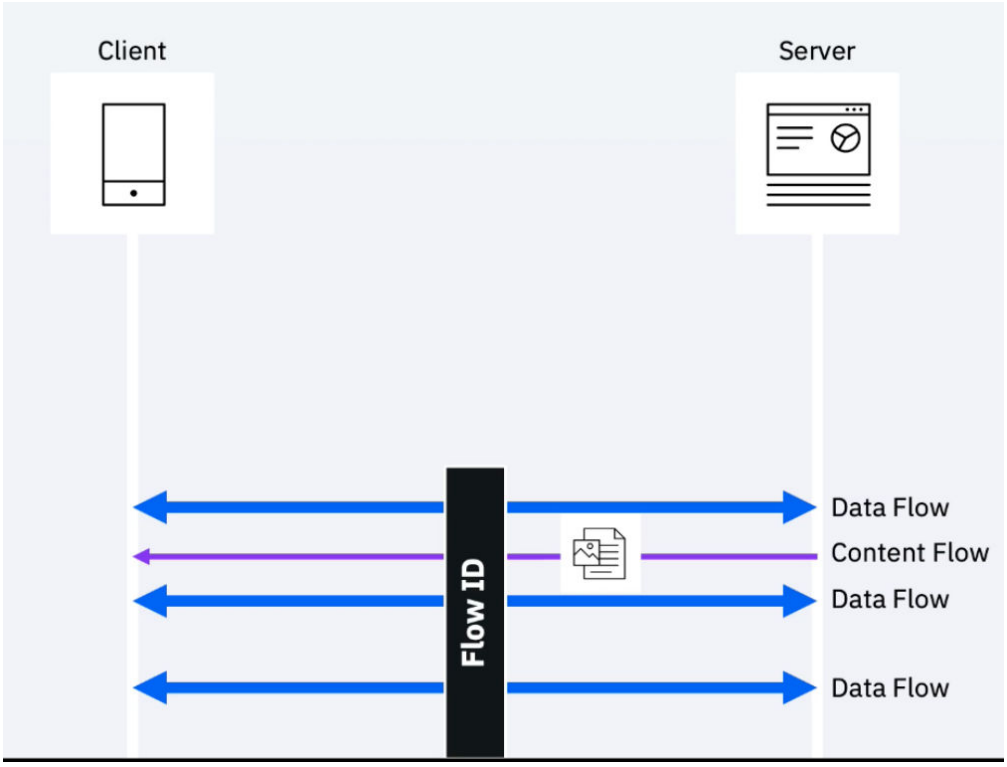
SUMMARY

Network Insights analyzes the network communication between a client and server. The communication is presented as data flows or content flows.

IN THIS SECTION

- Including Network Insights Data in Searches | **31**
- Identifying the Source of the Flow Data | **33**
- Parsing DNS Query and Response Fields | **34**
- Content Extensions | **36**

For example, consider a simple HTTP web connection. After the TCP handshake is negotiated, the client makes an HTTP request of the server. The server responds with an HTTP response. JSA Threat Analytics represents the communication between the client and server as bidirectional flow sessions. In cases where the flow session spans several minutes, JSA displays a summary flow record for each minute that the connection stays active. These flow records are linked by the **Flow ID** property, which provides a way to monitor all flow records that are part of the same session.



If you filter on **Flow Type**, both standard data flows and content flows appear in the filter results. When you create rules, you cannot use the **Flow Type** field as a distinction between data flows and content flows.

Data Flows

Data flows are traditional flow records. Also known as *standard flows*, they include payload samples, and show nonzero values in the byte and packet counters.

At the **Basic** inspection level, Network Insights creates only data flows. The data flow contains the same information as is collected by the QFlow process.

When you hover over the **Flow Type** column on the **Network Activity** tab, the tooltip for a data flow shows **Standard Flow**.

Content Flows

Content flows contain information that Network Insights collects at deeper levels of analysis and metadata extraction. Content flows do not include payload samples, and all byte and packet counters appear as zero.

The content flow is linked to the corresponding data flow by the `Flow ID` field. Network Insights creates content flows only when the inspection level is set to **Enriched** or **Advanced**.

When you hover over the **Flow Type** column on the **Network Activity** tab, the tooltip for a content flow shows **Standard Flow**.

Including Network Insights Data in Searches

SUMMARY

You can include Network Insights content in your data searches by including the content fields in the search criteria.

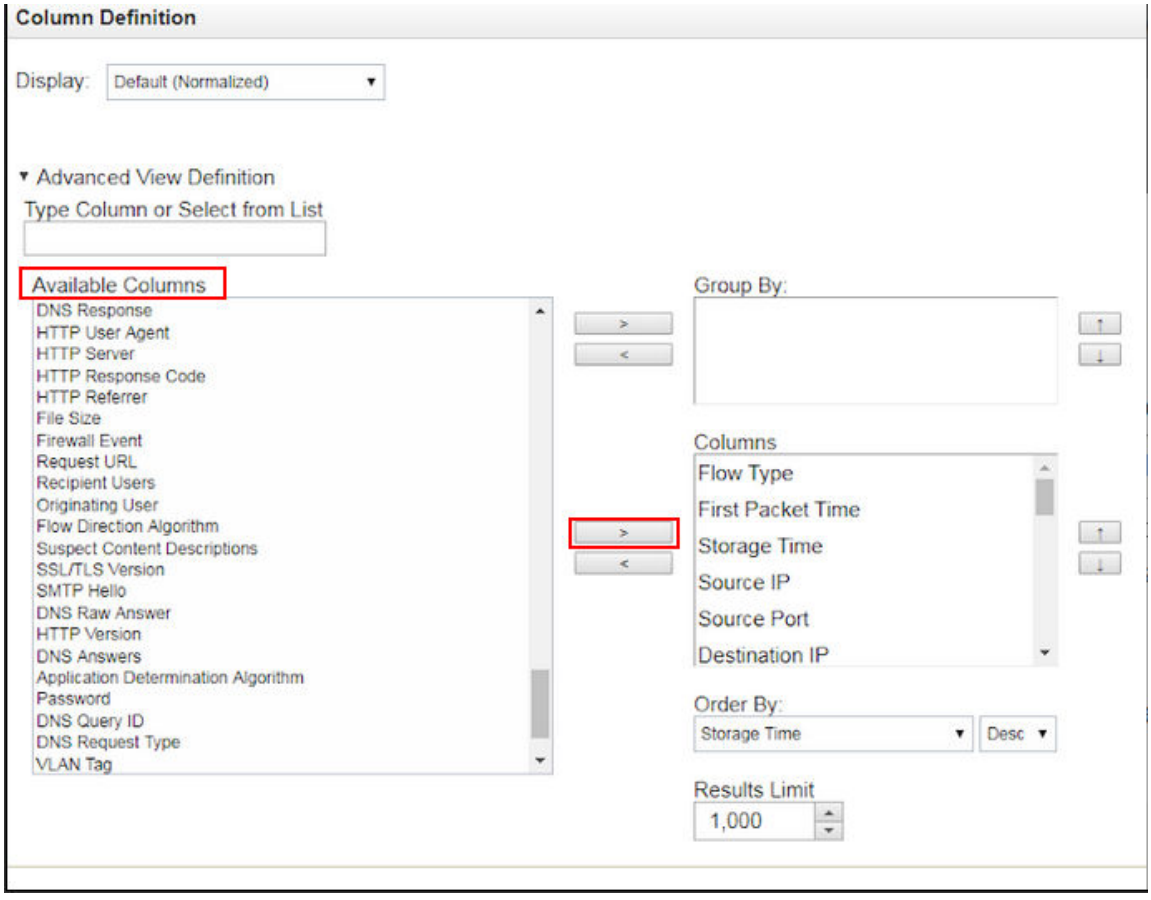
To ensure that flow inspection is configured to capture the content that you want to use, see Configuring the flow inspection level.

To find the name of the Network Insights content fields that you can search for, see the basic inspection level on page 15 and the enriched inspection level on page 17 content tables.

The name of the content field that you want to search for might differ depending on whether you search by using a regular search or an advanced search. If you want to do a regular search, use the `Query builder` name from the content tables. To run an advanced search, use the `Advanced Search` name.

1. To include the data fields in a regular search, complete the following steps:
   a. On the **Network Activity** tab, click **Search** > **New search**.
   b. In the **Column Definition** section, the **Available Columns** list shows the Network Insights data that you can include in your search results.
   c. To include the column in your query results, select the column from the list and then click the arrow to move the column to the **Columns** list.

Figure 1: Network Activity Tab Search View



For more information about searching by using the query builder, see Creating searches.

2. To include the data in an advanced search, follow these steps:

   a. On the **Network Activity** tab, click **Advanced Search**.

   b. In the **Advanced Search** box, type the Ariel Query Language (AQL) query that specifies the fields that you want and how you want to group them.

   For more information about creating advanced searches, see Advanced search options.

The flows that match the search criteria appear on the **Network Activity** tab. To view more information about the flow, double-click it to open the **Flow Information** window.

Identifying the Source of the Flow Data

The **Flow Source** and **Flow Interface** fields on the **Network Activity** tab can help you identify which Network Insights appliance that the flow was received from.

The **Flow Source** field shows the hostname of the managed host that received the flow.

The **Flow Interface** field shows the specific network interface that received the flows on the managed host. For standard network interfaces, the network interface name matches the names in the underlying Red Hat Enterprise Linux OS. For appliances with a Napatech card, the interface always appears as **napatech0**.

On the **Network Activity** tab, the flow source and flow interface appear in a single **Flow Source/Interface** field. In search results, the fields appear as two separate columns.

For example, the following image shows search results that include flows that are received from a Network Insights managed host with a hostname of *shortblack*. The flows are received from different network interfaces on the single appliance.

Application ▲	Source Bytes	Destinatio Bytes	Source Packets	Destination Packets	ICMP Type/Code	Flow Source	Flow Interface
DHCP.IPv6	156 (C)	0	1	0	N/A	shortblack	shortblack:eno2
DHCP.IPv6	483 (C)	0	3	0	N/A	shortblack	shortblack:napatech0
FileTransfer.NETBIOS	100 (C)	0	1	0	N/A	shortblack	shortblack:eno2
FileTransfer.NETBIOS	288 (C)	0	3	0	N/A	shortblack	shortblack:napatech0
FileTransfer.NETBIOS	100 (C)	0	1	0	N/A	shortblack	shortblack:eno2

1. Click the **Network Activity** tab.
2. In the toolbar, click the pause button to stop streaming the incoming flows.
3. Select the flow record that you want to view, and double-click to view the **Flow Information** window. The **Flow Source/Interface** field is shown at the bottom of the window, in the **Additional Information** section.

Parsing DNS Query and Response Fields

IN THIS SECTION

- DNS query | 34
- DNS Response | 35

The **DNS Query** and **DNS Response** fields were removed. You can still view the DNS response data by including more granular DNS data fields in your search results. For more information about the DNS data fields that you can use, see "Enriched Inspection" on page 16.

The following information can help you parse the data in the **DNS Query** and **DNS Response** fields. The **DNS Query** and **DNS Response** fields are populated only if the flow has data on a DNS query or DNS response, and the inspection level is set to **Enriched** or **Advanced**.

DNS query

The **DNS Query** field uses this format, which is described in the following table:

```
<transaction ID>,<flags>,<query domain>,<request type>
```

Table 3: Format for DNS Query Field

Field	Description
Transaction ID	Used by the DNS client and server to identify the transaction when it matches a request to a response.
Flags	A value of R indicates that recursion was requested; otherwise, the field is empty. When recursion is requested and enabled, the DNS server makes queries on behalf of the client to resolve the domain name.
Query domain	The domain name that was requested to be resolved.

Table 3: Format for DNS Query Field *(Continued)*

Field	Description
Request type	Identifies the type of resource information that was requested, as defined by the Internet Assigned Numbers Authority (IANA). Some of the most common requests types include IPv4 host address (A), IPv6 address (AAAA), canonical domain name for the alias (CNAME), the authoritative name server for the domain (NS), and name of the mail exchange server (MX).

For example, this DNS query is parsed like this:

```
51736,R,<domain name>,A
```

where

- The transaction ID is 51736.
- Recursion was requested.
- The bracketed location shows the domain name to be resolved.
- The resource information that is requested is the IPv4 host address.

DNS Response

The **DNS Response** field uses this format, which is described in the following table:

```
<transaction id>,<flags>,<query domain>,<response code>,
<num answers>,<num authority>,<num additional>,<answers>
```

Table 4: Format for DNS Response Field

Field	Description
Transaction ID	Used by the DNS client and server to identify the transaction when it matches a request to a response.

Table 4: Format for DNS Response Field *(Continued)*

Field	Description
Flags	Might be empty, or some combination of A,R, and T where • A means that the response is authoritative. • R means that recursion is available. • T means that the response was truncated.
Query domain	The domain name that was requested to be resolved.
Response code	A response code of 0 means that no errors were encountered. All other response code values indicate some type of error. For example, the query might be formatted improperly or the domain name might not exist.
Num answers	The number of regular answer records that were returned by the query.
Num authority	The number of authority answer records that were returned by the query.
Num additional	The number of extra answer records that were returned by the query.
Answers	The list of answer responses that were returned by the query. Each answer is separated by the "|" symbol. Authority and additional answers have the same format as regular answers, and are denoted as authority and additional answers based on their location in the answers list.

Content Extensions

Network Insights content extensions provide more JSA rules, reports, searches, and custom properties that you can use to perform deep analysis of network activity and application content.

To view a list of the content extensions that are available for Network Insights, see Network Insights Content Extensions.

For information about installing Network Insights content extensions, see Installing extensions by using Extensions Management.

6
CHAPTER

X-Force Integration

X-Force Integration in Network Insights | 38

X-Force Integration in Network Insights

IN THIS SECTION

- Suspect Content Descriptions Derived from X-Force | 38
- Flow property integration with X-Force Exchange | 40
- Direct Lookups for IP Reputation Classifications | 40

X-Force Exchange is a cloud-based threat intelligence platform that you can use to learn more about known global security threats and assess the potential threat to your network.

With built-in integration, Network Insights helps you use X-Force Exchange to identify and remediate undesirable activity in your environment before it threatens the stability of your network.

Network Insights analyzes the network communication between a client and server. The communication is presented as data flows or content flows.

Suspect Content Descriptions Derived from X-Force

IN THIS SECTION

- Suspect content descriptions in rules | 39

The IBM X-Force signature library includes descriptions for thousands of signatures.

At the enriched and advanced inspection level, Network Insights can detect suspicious content by using the X-Force signature library.

The signatures and issues are reported as suspect content on the **Network Activity** tab. The format for suspect content description depends on the information that is available.

- If the name of the detected issue ID is known, the suspect content description appears in the *XForceIssue <Name>* format.

For example, a named issue might appear as **XForceIssue Land_Attack**.

- If the name cannot be resolved for the detected issue, the issue ID appears in the suspect content description.

  For example, if the name cannot be identified, the issue might appear as **XForceIssueID 2000001**.

To learn more about the suspicious content, some fields on the **Flow information** window include direct links to view more information in X-Force Exchange.

To view a complete list of issues that are supported for the current deployment, view the **/opt/ibm/xforce/metadata/issues.csv** file on the Network Insights appliance.

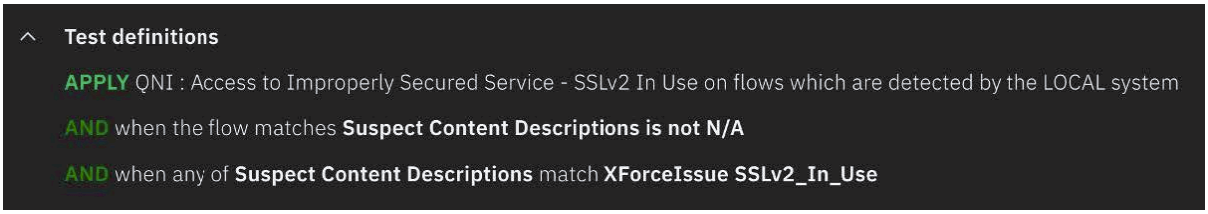
Suspect content descriptions in rules

For signatures that present a greater risk to your environment, create rules and offense notifications to help you detect and investigate these threats.

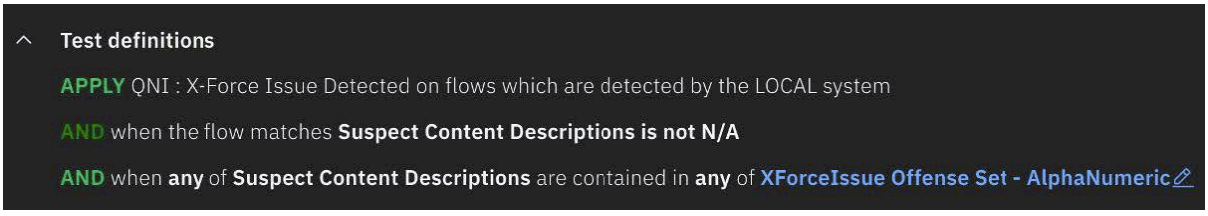
To determine which signatures to prioritize in your own environment, consider the following information:

- The use cases that are most relevant to your own environment.
- The signature priority as determined by IBM X-Force
- The moderate, aggressive, and paranoid issue policies that are defined in the **/opt/ibm/xforce/metadata** directory after the upgrade is complete.

When you use suspect content descriptions in rules, be specific with the signatures that you want to detect. This image shows an example rule that uses a suspect content description in the test criteria:



If you want to detect multiple signatures with a single rule, consider using a reference set.



Flow property integration with X-Force Exchange

Some flow properties in Network Insights are integrated with IBM X-Force Exchange to help you quickly determine whether the value requires further investigation.

On the **Flow Information** window, the following properties include links that you can click to open X-Force Exchange:

- TLS Server Name Indication
- HTTP Host
- DNS Domain Name
- File Hash
- MD5 File Hash
- SHA1 File Hash
- SHA256 File Hash
- Suspect content descriptions that come from the IBM X-Force signature library.

The following image shows some of the flow properties that are integrated with X-Force Exchange.

Direct Lookups for IP Reputation Classifications

To ensure that your IP reputation classifications are using the most recent classification information that is available, create rules and queries that use direct X-Force IP reputation lookups.

You can use the following X-Force IP categorizations:

- Anonymization Services
- Botnet Command and Control Server
- Bots
- Cryptocurrency Mining
- Dynamic IPs
- Malware
- Scanning IPs
- Spam

For example, a rule that uses the Anonymization Services categorization might use the following building block:

```
when Destination IP is categorized by X-Force as Anonymization Services with confidence value
greater than 50
```

In Ariel Query Language (AQL), you can use the *XFORCE_IP_CATEGORY* function instead.

CHAPTER 7

Supported Inspectors

Supported Inspectors | 43

Supported Inspectors

IN THIS SECTION

- Protocol Inspectors | 43
- Document Formats | 44
- Application Detection | 45

As network traffic data is processed and protocols are identified, the data is further inspected by the appropriate protocol and domain inspectors.

Protocol Inspectors

Protocol inspectors can identify protocols such as HTTP, POP3, FTP, and telnet. You can also exclude protocol inspectors. When the inspectors are excluded, any network traffic data that is associated with the inspector is still ingested, but the traffic is identified and indexed only on a generic level.
Any protocol that is not identifiable by a protocol inspector is categorized as **Unknown**.

The following list describes the supported protocols that Network Insights can process:

- AIM
- Berkeley remote commands (`rexec`, `rlogin`, `rsh`)
- BitTorrent
- DHCP
- DNS
- Exchange
- FTP
- HTTP
- iCAP
- IMAP

- IRC
- Jabber
- Kerberos
- MySQL
- MSN
- NFS
- NetBIOS Datagram (UDP)
- NetBIOS Session Service (TCP)
- NetBIOS Name Service (TCP)
- Oracle
- POP3
- Remote Desktop (RDP)
- SIP
- SMB (V1, V2, V3)
- SMTP
- SSH
- Telnet
- Trivial File Transfer Protocol (TFTP)
- TLS (SSL)
- Yahoo Messenger

Document Formats

SUMMARY

The following list describes the document formats that Network Insights can process:

- HyperText Markup Language
- XML and derived formats
- Microsoft Office document formats
- OpenDocument Format
- Portable Document Format
- Electronic Publication Format
- Rich Text Format
- Compression and packaging formats
- Text formats
- Audio formats
- Image formats
- Video formats
- Java class files and archives
- mbox format

Application Detection

IN THIS SECTION

- Application determination algorithms | 46

Network Insights uses inspectors to detect applications, sessions, and protocols.

JSA Network Insights 7.5.0 includes protocol parsing improvements and can now analyze the payload to identify approximately 300 more applications than earlier versions of the product.

To see the complete list of applications that JSA Network Insights 7.5.0 can identify, view these files after you upgrade.

- **/opt/ibm/xforce/metadata/protocols.hdr** (column headers)
- **/opt/ibm/xforce/metadata/protocols.csv** (values)

Application determination algorithms

Network Insights relies on its own set of inspectors and application detection methods. Network Insights, the Flow Processor algorithms are used only when Network Insights cannot identify a specific protocol.

The application determination algorithms are shown in the following table.

Table 5: Application determination algorithms

Numeric value	Algorithm name	Description
2	Application signatures	A payload-based algorithm that looks at the way that the payload is structured. This algorithm uses information from the **signatures.xml** file.
3	State-based decoding	A payload-based algorithm that uses complex internal logic.
4	JSA port-based mapping	A port-based algorithm that uses a pre-defined list of application mappings. This algorithm uses information from the **/opt/qradar/conf/appid_map.conf** file.

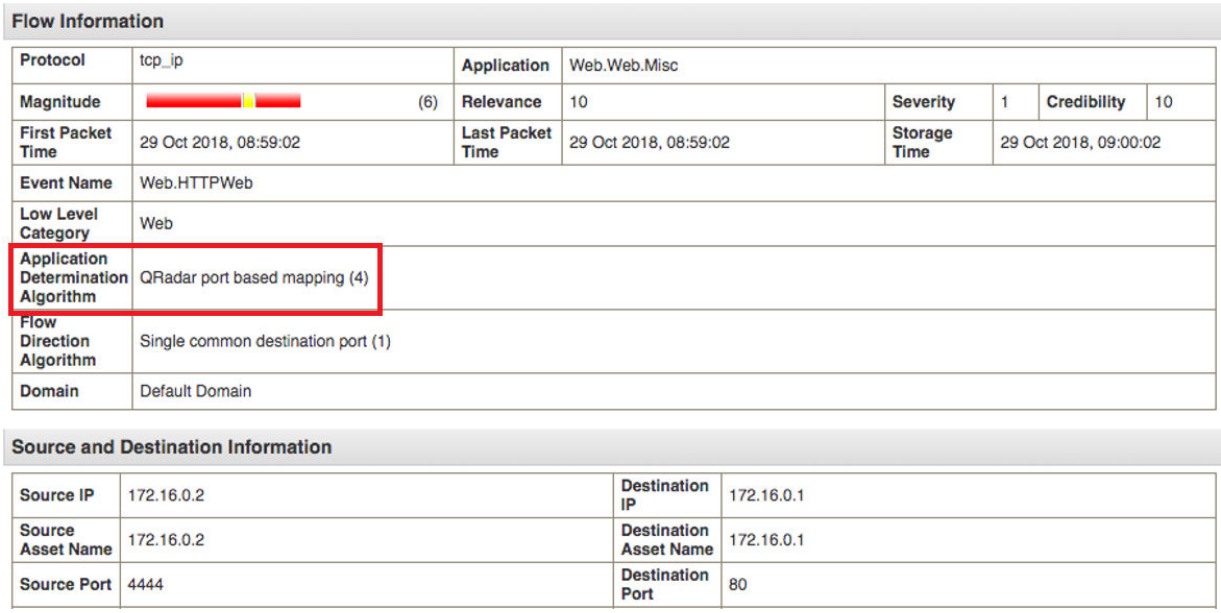
Table 5: Application determination algorithms *(Continued)*

Numeric value	Algorithm name	Description
5	User port-based mapping	A port-based algorithm that uses a customizable list of application mappings. Use this algorithm to add new port-based mappings or reclassify existing mappings that come with JSA. This algorithm uses information from the **/opt/qradar/conf/user_application_mapping.conf** file.
6	ICMP protocol mapping	A protocol-based algorithm that looks at the protocol type and code.
7	Flow exporter	An algorithm that relies on the Flow Exporter to determine the application. For example, the QFlow process inherently trusts application IDs that come from Network Insights.
8	QNI Application Signatures	This algorithm is used by Network Insights.
10	X-Force Web Application Classification	This algorithm is used by Network Insights.
11	QNI port heuristics	This algorithm is used by Network Insights. It indicates that the application is identified by using port-based heuristics, and represents a low degree of confidence.

Table 5: Application determination algorithms *(Continued)*

Numeric value	Algorithm name	Description
12	QNI initial data	This algorithm is used by Network Insights. It indicates that the application is identified by using the initial data in the flow session, and represents a medium degree of confidence.
13	QNI parsers	This algorithm is used by Network Insights. It indicates that the application is identified by parsing the available data, and represents the highest degree of confidence.

You can see which type of application detection algorithm that is used in the Application Determination Algorithm field on the Flow Information window.



Flow Information

Protocol	tcp_ip	**Application**	Web.Web.Misc				
Magnitude	(6)	**Relevance**	10	**Severity**	1	**Credibility**	10
First Packet Time	29 Oct 2018, 08:59:02	**Last Packet Time**	29 Oct 2018, 08:59:02	**Storage Time**	29 Oct 2018, 09:00:02		
Event Name	Web.HTTPWeb						
Low Level Category	Web						
Application Determination Algorithm	QRadar port based mapping (4)						
Flow Direction Algorithm	Single common destination port (1)						
Domain	Default Domain						

Source and Destination Information

Source IP	172.16.0.2	**Destination IP**	172.16.0.1
Source Asset Name	172.16.0.2	**Destination Asset Name**	172.16.0.1
Source Port	4444	**Destination Port**	80