List of application attributes LANShield can identify

Protocol identification is fundamentally necessary as a precursor to taking control of the LAN. To date this has been limited to Layer 3 and Layer 4 netflow and ACLs. However, changes in application design and vulnerabilities have altered the landscape, and enterprises today face increased security and control problems due to applications that port hop or share a common L4 port such as Port 80. These new risks illustrate why LAN infrastructure must provide and act on a far greater level of application intelligence. The next generation of LAN switches and routers use application intelligence to perform switching at L2,L3,L4,L7 & L7+ . ConSentry is the leader in high performance intelligent application identification. Below is the list of L7+ application attributes that can be identified and controlled via ConSentry LANShield OS. is the set of application attributes,

ConSentry has pioneered wirespeed Layer 7+ application decode in the LAN access layer. The company's patented LANShield silicon decodes applications at Layer 7 while maintaining 10 Gbps throughput – more than 5000% faster than competition. As a result, enterprises gain unprecedented visibility into and control over what users can do on the LAN. The LANShield OS 3.2 release supports the following Layer 7 application decodes.

Internet

- ***HTTP, Alternate HTTP***
  - Target Info
    - Host Name
  - Client/Server Info
    - User-Agent (Browser Type)
    - Server Name/Type
  - Content Info
    - HTTP Method (get, post, etc.)
    - HTTP URL
    - Content Type
  - Operation Error Info
    - Client/Server Error Responses

File Transfer & Services

- ***FTP***
  - Name Info
    - Login User Name
  - File Info
    - File Control/Transfer Operation
    - Filename (ASCII, UTF-8)
  - Operation Error Info
    - Transient Errors
    - Authentication/Accounting Errors
    - File System and Permanent Errors
- ***Microsoft SMB/CIFS***
  - Names and Client Info
    - Login User Names (ASCII, Unicode)
    - Client OS/Version
    - Client Hostname
    - Client Native LANManager
  - Connection Path Info
    - Connection/Tree Path Name (ASCII, Unicode)
  - File Access Info
    - File Access Operation (NTCreateX, OpenX, Delete, etc.)
    - Filename (ASCII, Unicode)
  - Operation Error Info
    - Session Setup/Authorization/Accounting Errors
    - Connection Path Errors
    - File Access Errors (open, create, delete, rename, etc.)

Client/Server

- ***SunRPC***
  - Remote Program Info
    - Portmapped Program Number

MS Windows, Windows Server

- ***MS-RPC/DCOM***
  - Remote Program Info
    - Endpoint-Mapped Program ID (UUID)

Voice over IP (VoIP)

- ***H.323 Videoconferencing***
  - Call Info
    - Calling and Called Party Numbers
    - Calling and Called Party Addresses
    - Call ID
- ***SIP***
  - Call Control Info
    - Session Control Operation (Invite, Ack, Bye)
    - Session Control URI
    - Informational/Success Response
    - Client/Server/Global Error Responses
  - Call Info
    - Called Party Name (To:)
    - Calling Party Name (From)
    - Calling User-Agent
    - Call ID
- ***RTP Streams***
  - Stream Type
    - H.323 Audio/Video/Data/Other
    - SIP Audio/Video/Data/Other
    - Cisco SCCP Audio/Video/Data
  - Codec Info
    - Audio - G.711, G.722, G.726, G.729, PCMU, etc.
    - Video - H.261, H.262, H.263, etc.
    - Data - T.120, T.84, etc.

Streaming Media

- ***Microsoft Media (Windows Media)***
  - Client Info
    - Media Player Program Name
    - Media Player Program Version #
  - Server Info
    - Media Server Version #
  - Payload Info
    - Payload Host Name
    - Payload Filename
- ***RTSP***
  - Server Info
    - Server Host Name
  - Payload Info
    - Payload Pathname
    - Payload Filename
    - Payload Stream #
- ***RTP Streams***
  - Stream Type
    - RTSP Audio/Video/Data
  - Codec Info
    - Audio - PCMU, DVI4, G.722, G.723, etc.
    - Video - H.261, H.263, JPEG, QuickTime, etc.
    - Data - Shockwave, RealNetworks Content, etc.

CONSENTRY NETWORKS

List of application attributes LANShield can identify

Instant Messaging, Chat

AOL IM (AIM)

- Names and Client Info
  - Client Screen Name
  - Connected Buddy Screen Names
  - Client Program Name
  - Client Program Version #
  - Client Country and Language
  - Client E-mail Address
- Logon Failure Info
  - Logon Error Reason
- File Transfer Info
  - Action Direction - Incoming vs. Outgoing
  - Transfer Direction - Send vs. Get
  - Transfer Mode - Service Start vs. Transfer Start
  - Transfer Type - File Transfer Service vs. Direct IM
  - Filename (ASCII, UTF-8)
- AIM Service Start Info
  - Known Services - File Transfer, Direct IM, Voice Chat, Video
  - Other Services (UUID)

Internet Relay Chat (IRC)

- Names and Client Info
  - Client Nickname
  - Client Realname
- Session Info
  - Local Domain (IRC User Mode)
  - Remote Domain (IRC User "unused", typical use)
  - Joined Channels

MS Messenger

- Names and Client Info
  - Client Screen Name
  - Session Buddy Screen Names
  - Client Program Version #
  - Client Type (Window vs. MSN/Windows Live Msgr)
- File Transfer Info
  - Action Direction - Incoming vs. Outgoing
  - Transfer Mode - Service Start vs. Transfer Start
  - Transfer Type - In-Band vs. Out-of-Band
  - Filename (ASCII, UTF-8, Unicode)

NateOn Messenger (Korea)

- Names and Client Info
  - Client Screen Name
  - Client Program Version #
- Logon Failure Info
  - Logon Error Reason
- Peer Activity Names
  - File Transfer Peer Screen Names
  - Audio Exchange Peer Screen Names

XMPP/Jabber/ GoogleTalk

- Names
  - Client Screen Name
  - Server Realm/Domain
- Logon Failure Info
  - Logon Error Reason
- Session Info
  - Client - Server vs. Server - Server
  - Clear vs. Encrypted
  - XMPP vs. Jabber vs. GoogleTalk

Yahoo! Messenger

- Names and Client Info
  - Client Screen Name
  - Client Given Name and Surname
  - Connected Buddy Screen Names
  - Client Program Version #
  - Client Locale (Language and Country)
- Logon Failure Info
  - Logon Error
- File Transfer Info
  - Action Direction - Incoming vs. Outgoing
  - Transfer Mode - Service Start vs. Transfer Start
  - Filename (ASCII)

Peer-to-Peer (P2P)

Various P2P Applications

- Client Info
  - User-Agent Name

Directory

DHCP

- Name Info
  - Host Name
  - Domain Name
  - User Class
  - Class Identifier
- Address Info
  - IP Address Lease Time
  - Router IP Address
  - Server IP Address
  - Subnet Mask

DNS

- Transaction Info
  - Transaction ID
  - Transaction Result - Success/Fail, including Fail Reason
- Answers Info
  - Queried Names
  - Queried Types, Classes, TTLs
  - Replied Values
- Authorities Info
  - Authority Names
  - Authority Types, Classes, TTLs
  - Authority Values
- Additional Items Info
  - Additional Item Names
  - Additional Item Types, Classes, TTLs
  - Additional Item Values

Microsoft Browser Protocol

- Browser Info
  - Browser Type (Host, Domain, Master, Local Master)
  - Host Name
  - Host Description
- Backup Browser Info
  - Backup Server Names List

Database, ERP

Oracle TNS

- Client Info
  - Client Program Name

Network Management

ICMP

- Control Info
  - Messaging Type (e.g. Echo, Domain, Trace Route, etc)