Application ID

Application ID

Traffic is commonly classified as a particular application or service using layer 4 port and protocol information. The Internet Assigned Numbers Authority (IANA) maintains a list of known service names, port numbers and protocols that are generally useful. Assuming applications and services adhere to the IANA convention and are trustworthy, use of this mapping would be sufficient when securing a network. In reality, applications and services can communicate using most any port, and when they have malicious intent, or are compromised to become malicious in intent, the use of layer 4 mappings for securing a network is insufficient.

Every application or service has a signature. When that signature is evaluated, the application or service can be classified more precisely. This classification is referred to as Application ID. When Application IDs are known, they can be used in a more advanced security posture to permit or block traffic, and to provide protections against malicious intent. Basic protection uses layer 4 information. More advanced protection uses Application ID information.

Multicloud Defense Application ID uses a set of capabilities for detecting and protecting applications and services:

- **IPS/IDS Profile** for enabling the Application ID detection engine.
- **Application Info** in Traffic Summary -> Logs for viewing the detected Application IDs for each session.
- **Service Object** for specifying the Application IDs to be used to match traffic.
- **Policy Ruleset Rule** for specifying the IDS/IPS Profile and the Service Object to enable detection and protection.

Note Application ID requires an IDS/IPS Profile to enable the Application ID detection engine. The Profile should be configured on all Policy Ruleset Rules where Application ID detection and protection is desired. It is a best practice to use IDS/IPS as part of an advanced security posture regardless of whether Application ID is used. It is recommended that an IDS/IPS Profile be configured for all Policy Ruleset Rules.

Application ID information can only be detected if the traffic is unencrypted and in clear form when using a Forwarding Service Object, or if encrypted traffic is decrypted when using a Decryption Profile in a Forward Proxy Service Object.

Specifying Application IDs

1. Navigate to **Manage** > **Security Policies** > **Services**.
2. Check the box next to an existing Forwarding or Forward Proxy Service Object and select **Edit** or create a new Forwarding or Forwarding Proxy Service Object by selecting **Create**.
3. In the Application IDs dropdown, select the relevant Application IDs.
4. Select **Save** to apply the Application ID settings.

If no Application IDs are specified, only layer 4 information (port and protocol) will be used to match. If Application IDs are specified, both layer 4 information and the Application ID information will be used to match. If more than one Application ID is specified an OR operator is applied.

Application ID Classification

There are four (4) classes of Application IDs. Client Application IDs are often applicable for Egress traffic. Legacy Application IDs are often applicable for East-West traffic. Cloud Service Application IDs are often applicable for Cloud Managed Service traffic. Miscellaneous Application IDs cover all other Application IDs that are often not in use in cloud environments, although can still be detected if the applications are in use.

Client Application IDs

Client Application IDs are often applicable for Egress traffic. This is the ID representing the client that is initiating the traffic. Some examples as shown below:

Application Category	Application IDs
Command line web utilities	Wget, cURL.
Browsers	Chrome, Firefox, Safari, Internet Explorer.
Packaging tools	Advanced Packaging Tool (apt), Windows Update, Microsoft Crypto API, urlgrabber, BITS.
Cloud utilities	AWS CLI
Edge	CloudFront

Legacy Application IDs

Legacy Application IDs are often applicable for East-West traffic. They usually represent applications that have been migrated from on-prem to public cloud in a lift-and-shift manor. Some examples as shown below:

Application Category	Application IDs
Interactive	SSH, Telnet, RDP
Databases	MSSQL, MySQL, PostgreSQL
File Server	SMBv2, SMBv3
Authentication	LDAP, LDAPS, Kerberos
Data Transfer	FTP Active, FTP Passive, TFTP
Communication	NETBIOS, RPC
Voice	SIP
Transport	HTTP, HTTPS
Name Resolution	DNS
Security	OCSP
Software Update	Microsoft Update, Office Mobile, Windows Live
Network Management	SNMPv1, SNMPv2c, SNMPv2u, SNMPv3
Encryption	TLS1.2, TLS1.3

Cloud Service Application IDs

Cloud Service Application IDs are often applicable for Cloud Managed Service traffic. Some examples of AWS managed services are shown below:

AWS Service Application ID
AWS Alexa
AWS Amplify
AWS Api Gateway
AWS Api Execute
AWS App AutoScaling
AWS App Stream2
AWS App Mesh
AWS App Sync

AWS Service Application ID
AWS Athena
AWS RDS
AWS Autoscaling Plans
AWS Backup
AWS Batch
AWS Budgets
AWS Savings Plans
AWS ACM
AWS Cloud9
AWS Cloud Dir
AWS Cloud Form
AWS Cloud HSMv2
AWS Cloud HSM
AWS Svc Disc
AWS Cloud Srch
AWS Cloud Trail
AWS Cloud Watch
AWS Events
AWS Logs
AWS Synthetics
AWS Code Artfct
AWS Code Build
AWS Code Commit
AWS Code Deploy
AWS Code Profile
AWS Code Review
AWS Code Pipeline
AWS Code Star

AWS Service Application ID
AWS Code Star Notifications
AWS Cognito IDP
AWS Cognito Identity
AWS Cognito Sync
AWS Comprehend
AWS Comprehend Medical
AWS Compute Optimizer
AWS Config
AWS Connect
AWS Data Exchange
AWS DLM
AWS Data Pipeline
AWS Data Sync
AWS DMS
AWS Detective
AWS Devops Guru
AWS Direct Connect
AWS DS
AWS Dynamo DB
AWS DAX
AWS Streams
AWS Elastic Beanstalk
AWS Elastic Compute
AWS Elastic Block Storage
AWS Image Builder
AWS ECR
AWS ECS
AWS EKS

AWS Service Application ID
AWS EFS
AWS Elastic Inference
AWS Elastic Transcoder
AWS Elastic Cache
AWS ES
AWS Elastic Map Reduce
AWS FMS
AWS Forecast
AWS Fraud Detector
AWS IoT
AWS FSX
AWS Gamelift
AWS Glacier
AWS Global Accelerator
AWS Glue
AWS Ground Station
AWS Guard Duty
AWS Health
AWS IAM
AWS Access Analyzer
AWS Import Export
AWS Inspector
AWS IoT1click
AWS IoT Analytics
AWS Data
AWS Tunnelling
AWS Jobs
AWS IoT Events

AWS Service Application ID
AWS Greengrass
AWS Prefix ATS
AWS Greengrass ATS
AWS IoT Sitewise
AWS IoT Things Graph
AWS KMS
AWS Kinesis Analytics
AWS Firehose
AWS Kinesis
AWS Kinesis Video
AWS Lake Formation
AWS Lambda
AWS App Wizard
AWS Models
AWS Runtime
AWS License Manager
AWS Lightsail
AWS Macie2
AWS Macie
AWS Machine Learning
AWS Managed Blockchain
AWS Metering
AWS Mturk
AWS Kafka
AWS Media Connect
AWS Media Convert
AWS Media Package
AWS Media Store

AWS Service Application ID
AWS Media Tailor
AWS MGH
AWS MQ
AWS Network Firewall
AWS Network Manager
AWS Opsworks
AWS Organizations
AWS Outposts
AWS Pinpoint
AWS SMS Voice
AWS Polly
AWS Qldb
AWS Quicksight
AWS Ram
AWS Redshift
AWS Rekognition
AWS Pi
AWS Resource Groups
AWS Tagging
AWS Robomaker
AWS Route53
AWS Route53 Domains
AWS Route53 Resolver
AWS Sagemaker
AWS Secrets Manager
AWS Security Hub
AWS STS
AWS SMS

AWS Service Application ID
AWS Service Quotas
AWS Serverless Repo
AWS Service Catalog
AWS Shield
AWS SNS
AWS SQS
AWS Queue
AWS SWF
AWS SDB
AWS SSO
AWS Identity Store
AWS Snowball
AWS States
AWS Storage Gateway
AWS Support
AWS SSM
AWS Textract
AWS Transcribe
AWS Transfer
AWS Translate
AWS WAFv2
AWS WAF
AWS Workdocs
AWS Workspaces
AWS X Ray
AWS Elastic Load Balancing
AWS Messaging

Example Application ID Sets

A few common sets of Application IDs are shown below:

Active Directory

Set of Application IDs for Active Directory

Application ID
LDAP
Kerberos
NETBIOS
SMBv2
SMBv3
DNS
NetBIOS-ns
DCE/RPC
MySQL

Windows Update

Set of Application IDs for Windows Update

Application ID
Microsoft Update
Windows Update
Microsoft CryptoAPI
BITS
Office Mobile
Windows Live

Centos or Ubuntu Install

Set of Application IDs for Centos or Ubuntu Install

Application ID
Advanced Packaging Tool
urlgrabber
BITS
CloudFront
HTTP
HTTPS
GIOP
DAAP