애플리케이션 ID

애플리케이션 ID

트래픽은 일반적으로 레이어 4 포트 및 프로토콜 정보를 사용하여 특정 애플리케이션 또는 서비스로 분류됩니다. IANA(Internet Assigned Numbers Authority)에서는 일반적으로 유용한 알려진 서비스 이름, 포트 번호, 프로토콜의 목록을 유지 관리합니다. 애플리케이션 및 서비스가 IANA 규칙을 준수하고 신뢰할 수 있다고 가정할 때 네트워크 보안 시 이 매핑만 사용하면 충분할 것입니다. 실제로 애플리케이션과 서비스는 거의 모든 포트를 사용하여 통신할 수 있으며, 악의적인 의도를 가지고 있거나 악의적인 의도로 손상된 경우 네트워크 보안을 위한 레이어 4 매핑을 사용하는 것만으로는 충분하지 않습니다.

모든 애플리케이션 또는 서비스에는 서명이 있습니다. 해당 서명이 평가되면 애플리케이션 또는 서비스를 더욱 정확하게 분류할 수 있습니다. 이 분류를 애플리케이션 ID라고 합니다. 애플리케이션 ID가 알려진 경우, 고급 보안 태세에서 이를 사용하여 트래픽을 허용 또는 차단하고 악의적인 의도로부터 보호할 수 있습니다. 기본 보호는 레이어 4 정보를 사용합니다. 고급 보호 기능에서는 애플리케이션 ID 정보를 사용합니다.

멀티 클라우드 방어 애플리케이션 ID는 애플리케이션과 서비스를 탐지하고 보호하기 위해 일련의 기능을 사용합니다.

- 애플리케이션 ID 탐지 엔진 활성화를 위한 **IPS/IDS** 프로파일.
- 각 세션에 대해 감지된 애플리케이션 ID를 보기 위한 트래픽 요약 -> 로그의 애플리케이션 정보.
- 트래픽 일치에 사용할 애플리케이션 ID를 지정하기 위한 서비스 개체.
- 탐지 및 보호를 활성화하기 위한 IDS/IPS 프로파일 및 서비스 개체를 지정하는 정책 규칙 집합 규칙.

Note 애플리케이션 ID를 사용하려면 애플리케이션 ID 탐지 엔진을 활성화하는 IDS/IPS 프로파일이 필요합니다. 애플리케이션 ID 탐지 및 보호가 필요한 모든 정책 규칙 집합 규칙에서 프로파일을 구성해야 합니다. 애플리케이션 ID의 사용 여부에 관계없이 고급 보안 태세의 일부로 IDS/IPS를 사용하는 것이 모범 사례입니다. 모든 정책 규칙 집합 규칙에 대해 IDS/IPS 프로파일을 구성하는 것이 좋습니다.

애플리케이션 ID 정보는 전달 서비스 개체를 사용할 때 트래픽이 암호화되지 않고 일반 형식인 경우, 또는 정방향 프록시 서비스 개체의 암호 해독 프로파일을 사용할 때 암호화된 트래픽이 암호 해독된 경우에만 탐지할 수 있습니다.

애플리케이션 ID 지정

1. **Manage(**관리**)** > **Security Policies(**보안 정책**)** > **Services(**서비스**)**로 이동합니다.
2. 기존 전달 또는 전달 프록시 서비스 개체 옆에 있는 확인란을 선택하고 **Edit(**편집**)**을 선택하거나 **Create(**생성**)**을 선택하여 새 전달 또는 전달 프록시 서비스 개체를 생성합니다.
3. Application IDs(애플리케이션 ID) 드롭다운에서 관련 애플리케이션 ID를 선택합니다.
4. **Save(**저장**)**를 선택하여 애플리케이션 ID 설정을 적용합니다.

애플리케이션 ID가 지정되지 않은 경우, 레이어 4 정보(포트 및 프로토콜)만 일치에 사용됩니다. 애플리케이션 ID를 지정하면 레이어 4 정보와 애플리케이션 ID 정보를 모두 사용하여 일치시킵니다. 둘 이상의 애플리케이션 ID가 지정된 경우 OR 연산자가 적용됩니다.

애플리케이션 ID 분류

애플리케이션 ID에는 4개의 클래스가 있습니다. 클라이언트 애플리케이션 ID는 종종 이그레스 트래픽에 적용됩니다. 레거시 애플리케이션 ID는 종종 이스트-웨스트 트래픽에 적용됩니다. 클라우드 서비스 애플리케이션 ID는 종종 클라우드 관리 서비스 트래픽에 적용됩니다. 기타 애플리케이션 ID는 애플리케이션이 사용 중인 경우 계속 탐지될 수 있지만 클라우드 환경에서 자주 사용되지 않는 다른 모든 애플리케이션 ID에 적용됩니다.

클라이언트 애플리케이션 ID

클라이언트 애플리케이션 ID는 종종 이그레스 트래픽에 적용됩니다. 이는 트래픽을 시작하는 클라이언트를 나타내는 ID입니다. 몇 가지 예를 들면 다음과 같습니다.

애플리케이션 범주	애플리케이션 ID
명령줄 웹 유틸리티	Wget, cURL.
브라우저	Chrome, Firefox, Safari, Internet Explorer.

애플리케이션 범주	애플리케이션 ID
패키징 툴	고급 패키징 툴(apt), Windows 업데이트, Microsoft Crypto API, urlgrabber, BITS.
클라우드 유틸리티	AWS CLI
Edge	CloudFront

레거시 애플리케이션 ID

레거시 애플리케이션 ID는 종종 이스트-웨스트 트래픽에 적용됩니다. 일반적으로 온프레미스에서 퍼블릭 클라우드로 마이그레이션된 애플리케이션을 나타냅니다. 몇 가지 예를 들면 다음과 같습니다.

애플리케이션 범주	애플리케이션 ID
대화형	SSH, Telnet, RDP
데이터베이스	MSSQL, MySQL, PostgreSQL
파일 서버	SMBv2, SMBv3
인증	LDAP, LDAPS, Kerberos
데이터 전송	FTP 액티브, FTP 패시브, TFTP
의사소통	NETBIOS, RPC
음성	SIP
전송	HTTP, HTTPS
이름 확인	DNS
보안	OCSP
소프트웨어 업데이트	Microsoft Update, Office Mobile, Windows Live
네트워크 관리	SNMPv1, SNMPv2c, SNMPv2u, SNMPv3
암호화	TLS1.2, TLS1.3

클라우드 서비스 애플리케이션 ID

클라우드 서비스 애플리케이션 ID는 종종 클라우드 관리 서비스 트래픽에 적용됩니다. AWS 관리 서비스의 몇 가지 예시가 아래에 나와 있습니다.

AWS 서비스 애플리케이션 **ID**
AWS Alexa
AWS Amplify
AWS Api Gateway
AWS Api Execute
AWS App AutoScaling
AWS App Stream2
AWS App Mesh
AWS App Sync
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 서비스 애플리케이션 **ID**
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 Code Star Notifications
AWS Cognito IDP
AWS Cognito ID
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 서비스 애플리케이션 **ID**
AWS Streams
AWS Elastic Beanstalk
AWS Elastic Compute
AWS Elastic Block Storage
AWS Image Builder
AWS ECR
AWS ECS
AWS EKS
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 서비스 애플리케이션 **ID**
AWS Import Export
AWS Inspector
AWS IoT1click
AWS IoT Analytics
AWS Data
AWS Tunnelling
AWS Jobs
AWS IoT Events
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 서비스 애플리케이션 **ID**
AWS Managed Blockchain
AWS Metering
AWS Mturk
AWS Kafka
AWS Media Connect
AWS Media Convert
AWS Media Package
AWS Media Store
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 서비스 애플리케이션 **ID**
AWS Route53
AWS Route53 Domains
AWS Route53 Resolver
AWS Sagemaker
AWS Secrets Manager
AWS Security Hub
AWS STS
AWS SMS
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 Texttract
AWS Transcribe
AWS Transfer
AWS Translate

AWS 서비스 애플리케이션 ID
AWS WAFv2
AWS WAF
AWS Workdocs
AWS Workspaces
AWS X Ray
AWS Elastic Load Balancing
AWS Messaging

애플리케이션 ID 세트 예

애플리케이션 ID의 몇 가지 일반적인 집합은 다음과 같습니다.

Active Directory

Active Directory용 애플리케이션 ID 집합

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

Windows 업데이트

Windows 업데이트용 애플리케이션 ID 집합

애플리케이션 ID
Microsoft 업데이트

애플리케이션 ID
Windows 업데이트
Microsoft CryptoAPI
BITS
Office Mobile
Windows Live

Centos 또는 Ubuntu 설치

Centos 또는 Ubuntu 설치용 애플리케이션 ID 집합

애플리케이션 ID
고급 패키징 툴
urlgrabber
BITS
CloudFront
HTTP
HTTPS
GIOP
DAAP