#패킷처리 단계(New Session)

1. **초기 패킷 처리** : Source 존&주소/유저 ID > PBR/포워딩 조회 > Destination 존 > NAT 정책 평가
2. **사전 보안 정책** : 허용 포트 확인 > 세션 생성(6-tuple : 소스 IP/소스 존/대상 IP/대상 존/대상 포트/프로토콜)
3. **애플리케이션** : 암호화 확인 > 복호화 정책 조회 > 애플리케이션 오버라이드 정책 > App-ID/Content-ID 라벨 지정
4. **보안 정책** : 보안 정책 확인 > 보안 프로파일 확인
5. **사후 정책 처리** : 트래픽 재암호화 > NAT 정책 적용 > 패킷 포워딩

#App-ID 분류 방법

패킷 수신 > 6-Tuple 확인 > 보안 정책 확인 > 알려진 애플리케이션 시그니처 확인 *애플리케이션 식별 작업 >

1. 보안 정책 재확인 > 더이상 디코딩이 필요하지 않은 세션 식별
2. 보안 정책 재확인 > SSH 또는 TLS 암호 해독 *복호화 >애플리케이션 식별 작업
3. 보안 정책 재확인 > 알수없는 프로토콜 : 휴리스틱 적용
4. 보안 정책 재확인 > 알려진 프로토콜 : 디코드

#패킷처리 단계(New Session)

1. **초기 패킷 처리** : Source 존&주소/유저 ID > PBR/포워딩 조회 > Destination 존 > NAT 정책 평가
2. **사전 보안 정책** : 허용 포트 확인 > 세션 생성(6-tuple : 소스 IP/소스 존/대상 IP/대상 존/대상 포트/프로토콜)
3. **애플리케이션** : 암호화 확인 > 복호화 정책 조회 > 애플리케이션 오버라이드 정책 > App-ID/Content-ID 라벨 지정
4. **보안 정책** : 보안 정책 확인 > 보안 프로파일 확인
5. **사후 정책 처리** : 트래픽 재암호화 > NAT 정책 적용 > 패킷 포워딩

#App-ID 분류 방법

패킷 수신 > 6-Tuple 확인 > 보안 정책 확인 > 알려진 애플리케이션 시그니처 확인 *애플리케이션 식별 작업 >

1. 보안 정책 재확인 > 더이상 디코딩이 필요하지 않은 세션 식별
2. 보안 정책 재확인 > SSH 또는 TLS 암호 해독 *복호화 >애플리케이션 식별 작업
3. 보안 정책 재확인 > 알수없는 프로토콜 : 휴리스틱 적용
4. 보안 정책 재확인 > 알려진 프로토콜 : 디코드

#패킷처리 단계(New Session)

1. **초기 패킷 처리** : Source 존&주소/유저 ID > PBR/포워딩 조회 > Destination 존 > NAT 정책 평가
2. **사전 보안 정책** : 허용 포트 확인 > 세션 생성(6-tuple : 소스 IP/소스 존/대상 IP/대상 존/대상 포트/프로토콜)
3. **애플리케이션** : 암호화 확인 > 복호화 정책 조회 > 애플리케이션 오버라이드 정책 > App-ID/Content-ID 라벨 지정
4. **보안 정책** : 보안 정책 확인 > 보안 프로파일 확인
5. **사후 정책 처리** : 트래픽 재암호화 > NAT 정책 적용 > 패킷 포워딩

#App-ID 분류 방법

패킷 수신 > 6-Tuple 확인 > 보안 정책 확인 > 알려진 애플리케이션 시그니처 확인 *애플리케이션 식별 작업 >

1. 보안 정책 재확인 > 더이상 디코딩이 필요하지 않은 세션 식별
2. 보안 정책 재확인 > SSH 또는 TLS 암호 해독 *복호화 >애플리케이션 식별 작업
3. 보안 정책 재확인 > 알수없는 프로토콜 : 휴리스틱 적용
4. 보안 정책 재확인 > 알려진 프로토콜 : 디코드

#패킷처리 단계(New Session)

1. **초기 패킷 처리** : Source 존&주소/유저 ID > PBR/포워딩 조회 > Destination 존 > NAT 정책 평가
2. **사전 보안 정책** : 허용 포트 확인 > 세션 생성(6-tuple : 소스 IP/소스 존/대상 IP/대상 존/대상 포트/프로토콜)
3. **애플리케이션** : 암호화 확인 > 복호화 정책 조회 > 애플리케이션 오버라이드 정책 > App-ID/Content-ID 라벨 지정
4. **보안 정책** : 보안 정책 확인 > 보안 프로파일 확인
5. **사후 정책 처리** : 트래픽 재암호화 > NAT 정책 적용 > 패킷 포워딩

#App-ID 분류 방법

패킷 수신 > 6-Tuple 확인 > 보안 정책 확인 > 알려진 애플리케이션 시그니처 확인 *애플리케이션 식별 작업 >

1. 보안 정책 재확인 > 더이상 디코딩이 필요하지 않은 세션 식별
2. 보안 정책 재확인 > SSH 또는 TLS 암호 해독 *복호화 >애플리케이션 식별 작업
3. 보안 정책 재확인 > 알수없는 프로토콜 : 휴리스틱 적용
4. 보안 정책 재확인 > 알려진 프로토콜 : 디코드

#패킷처리 단계(New Session)

1. **초기 패킷 처리** : Source 존&주소/유저 ID > PBR/포워딩 조회 > Destination 존 > NAT 정책 평가
2. **사전 보안 정책** : 허용 포트 확인 > 세션 생성(6-tuple : 소스 IP/소스 존/대상 IP/대상 존/대상 포트/프로토콜)
3. **애플리케이션** : 암호화 확인 > 복호화 정책 조회 > 애플리케이션 오버라이드 정책 > App-ID/Content-ID 라벨 지정
4. **보안 정책** : 보안 정책 확인 > 보안 프로파일 확인
5. **사후 정책 처리** : 트래픽 재암호화 > NAT 정책 적용 > 패킷 포워딩

#App-ID 분류 방법

패킷 수신 > 6-Tuple 확인 > 보안 정책 확인 > 알려진 애플리케이션 시그니처 확인 *애플리케이션 식별 작업 >

1. 보안 정책 재확인 > 더이상 디코딩이 필요하지 않은 세션 식별
2. 보안 정책 재확인 > SSH 또는 TLS 암호 해독 *복호화 >애플리케이션 식별 작업
3. 보안 정책 재확인 > 알수없는 프로토콜 : 휴리스틱 적용
4. 보안 정책 재확인 > 알려진 프로토콜 : 디코드

#패킷처리 단계(New Session)

1. **초기 패킷 처리** : Source 존&주소/유저 ID > PBR/포워딩 조회 > Destination 존 > NAT 정책 평가
2. **사전 보안 정책** : 허용 포트 확인 > 세션 생성(6-tuple : 소스 IP/소스 존/대상 IP/대상 존/대상 포트/프로토콜)
3. **애플리케이션** : 암호화 확인 > 복호화 정책 조회 > 애플리케이션 오버라이드 정책 > App-ID/Content-ID 라벨 지정
4. **보안 정책** : 보안 정책 확인 > 보안 프로파일 확인
5. **사후 정책 처리** : 트래픽 재암호화 > NAT 정책 적용 > 패킷 포워딩

#App-ID 분류 방법

패킷 수신 > 6-Tuple 확인 > 보안 정책 확인 > 알려진 애플리케이션 시그니처 확인 *애플리케이션 식별 작업 >

1. 보안 정책 재확인 > 더이상 디코딩이 필요하지 않은 세션 식별
2. 보안 정책 재확인 > SSH 또는 TLS 암호 해독 *복호화 >애플리케이션 식별 작업
3. 보안 정책 재확인 > 알수없는 프로토콜 : 휴리스틱 적용
4. 보안 정책 재확인 > 알려진 프로토콜 : 디코드

#패킷처리 단계(New Session)

1. **초기 패킷 처리** : Source 존&주소/유저 ID > PBR/포워딩 조회 > Destination 존 > NAT 정책 평가
2. **사전 보안 정책** : 허용 포트 확인 > 세션 생성(6-tuple : 소스 IP/소스 존/대상 IP/대상 존/대상 포트/프로토콜)
3. **애플리케이션** : 암호화 확인 > 복호화 정책 조회 > 애플리케이션 오버라이드 정책 > App-ID/Content-ID 라벨 지정
4. **보안 정책** : 보안 정책 확인 > 보안 프로파일 확인
5. **사후 정책 처리** : 트래픽 재암호화 > NAT 정책 적용 > 패킷 포워딩

#App-ID 분류 방법

패킷 수신 > 6-Tuple 확인 > 보안 정책 확인 > 알려진 애플리케이션 시그니처 확인 *애플리케이션 식별 작업 >

1. 보안 정책 재확인 > 더이상 디코딩이 필요하지 않은 세션 식별
2. 보안 정책 재확인 > SSH 또는 TLS 암호 해독 *복호화 >애플리케이션 식별 작업
3. 보안 정책 재확인 > 알수없는 프로토콜 : 휴리스틱 적용
4. 보안 정책 재확인 > 알려진 프로토콜 : 디코드

#패킷처리 단계(New Session)

1. **초기 패킷 처리** : Source 존&주소/유저 ID > PBR/포워딩 조회 > Destination 존 > NAT 정책 평가
2. **사전 보안 정책** : 허용 포트 확인 > 세션 생성(6-tuple : 소스 IP/소스 존/대상 IP/대상 존/대상 포트/프로토콜)
3. **애플리케이션** : 암호화 확인 > 복호화 정책 조회 > 애플리케이션 오버라이드 정책 > App-ID/Content-ID 라벨 지정
4. **보안 정책** : 보안 정책 확인 > 보안 프로파일 확인
5. **사후 정책 처리** : 트래픽 재암호화 > NAT 정책 적용 > 패킷 포워딩

#App-ID 분류 방법

패킷 수신 > 6-Tuple 확인 > 보안 정책 확인 > 알려진 애플리케이션 시그니처 확인 *애플리케이션 식별 작업 >

1. 보안 정책 재확인 > 더이상 디코딩이 필요하지 않은 세션 식별
2. 보안 정책 재확인 > SSH 또는 TLS 암호 해독 *복호화 >애플리케이션 식별 작업
3. 보안 정책 재확인 > 알수없는 프로토콜 : 휴리스틱 적용
4. 보안 정책 재확인 > 알려진 프로토콜 : 디코드

#패킷처리 단계(New Session)

1. **초기 패킷 처리** : Source 존&주소/유저 ID > PBR/포워딩 조회 > Destination 존 > NAT 정책 평가
2. **사전 보안 정책** : 허용 포트 확인 > 세션 생성(6-tuple : 소스 IP/소스 존/대상 IP/대상 존/대상 포트/프로토콜)
3. **애플리케이션** : 암호화 확인 > 복호화 정책 조회 > 애플리케이션 오버라이드 정책 > App-ID/Content-ID 라벨 지정
4. **보안 정책** : 보안 정책 확인 > 보안 프로파일 확인
5. **사후 정책 처리** : 트래픽 재암호화 > NAT 정책 적용 > 패킷 포워딩

#App-ID 분류 방법

패킷 수신 > 6-Tuple 확인 > 보안 정책 확인 > 알려진 애플리케이션 시그니처 확인 *애플리케이션 식별 작업 >

1. 보안 정책 재확인 > 더이상 디코딩이 필요하지 않은 세션 식별
2. 보안 정책 재확인 > SSH 또는 TLS 암호 해독 *복호화 >애플리케이션 식별 작업
3. 보안 정책 재확인 > 알수없는 프로토콜 : 휴리스틱 적용
4. 보안 정책 재확인 > 알려진 프로토콜 : 디코드

#패킷처리 단계(New Session)

1. **초기 패킷 처리** : Source 존&주소/유저 ID > PBR/포워딩 조회 > Destination 존 > NAT 정책 평가
2. **사전 보안 정책** : 허용 포트 확인 > 세션 생성(6-tuple : 소스 IP/소스 존/대상 IP/대상 존/대상 포트/프로토콜)
3. **애플리케이션** : 암호화 확인 > 복호화 정책 조회 > 애플리케이션 오버라이드 정책 > App-ID/Content-ID 라벨 지정
4. **보안 정책** : 보안 정책 확인 > 보안 프로파일 확인
5. **사후 정책 처리** : 트래픽 재암호화 > NAT 정책 적용 > 패킷 포워딩

#App-ID 분류 방법

패킷 수신 > 6-Tuple 확인 > 보안 정책 확인 > 알려진 애플리케이션 시그니처 확인 *애플리케이션 식별 작업 >

1. 보안 정책 재확인 > 더이상 디코딩이 필요하지 않은 세션 식별
2. 보안 정책 재확인 > SSH 또는 TLS 암호 해독 *복호화 >애플리케이션 식별 작업
3. 보안 정책 재확인 > 알수없는 프로토콜 : 휴리스틱 적용
4. 보안 정책 재확인 > 알려진 프로토콜 : 디코드

#패킷처리 단계(New Session)

1. **초기 패킷 처리** : Source 존&주소/유저 ID > PBR/포워딩 조회 > Destination 존 > NAT 정책 평가
2. **사전 보안 정책** : 허용 포트 확인 > 세션 생성(6-tuple : 소스 IP/소스 존/대상 IP/대상 존/대상 포트/프로토콜)
3. **애플리케이션** : 암호화 확인 > 복호화 정책 조회 > 애플리케이션 오버라이드 정책 > App-ID/Content-ID 라벨 지정
4. **보안 정책** : 보안 정책 확인 > 보안 프로파일 확인
5. **사후 정책 처리** : 트래픽 재암호화 > NAT 정책 적용 > 패킷 포워딩

#App-ID 분류 방법

패킷 수신 > 6-Tuple 확인 > 보안 정책 확인 > 알려진 애플리케이션 시그니처 확인 *애플리케이션 식별 작업 >

1. 보안 정책 재확인 > 더이상 디코딩이 필요하지 않은 세션 식별
2. 보안 정책 재확인 > SSH 또는 TLS 암호 해독 *복호화 >애플리케이션 식별 작업
3. 보안 정책 재확인 > 알수없는 프로토콜 : 휴리스틱 적용
4. 보안 정책 재확인 > 알려진 프로토콜 : 디코드

#패킷처리 단계(New Session)

1. **초기 패킷 처리** : Source 존&주소/유저 ID > PBR/포워딩 조회 > Destination 존 > NAT 정책 평가
2. **사전 보안 정책** : 허용 포트 확인 > 세션 생성(6-tuple : 소스 IP/소스 존/대상 IP/대상 존/대상 포트/프로토콜)
3. **애플리케이션** : 암호화 확인 > 복호화 정책 조회 > 애플리케이션 오버라이드 정책 > App-ID/Content-ID 라벨 지정
4. **보안 정책** : 보안 정책 확인 > 보안 프로파일 확인
5. **사후 정책 처리** : 트래픽 재암호화 > NAT 정책 적용 > 패킷 포워딩

#App-ID 분류 방법

패킷 수신 > 6-Tuple 확인 > 보안 정책 확인 > 알려진 애플리케이션 시그니처 확인 *애플리케이션 식별 작업 >

1. 보안 정책 재확인 > 더이상 디코딩이 필요하지 않은 세션 식별
2. 보안 정책 재확인 > SSH 또는 TLS 암호 해독 *복호화 >애플리케이션 식별 작업
3. 보안 정책 재확인 > 알수없는 프로토콜 : 휴리스틱 적용
4. 보안 정책 재확인 > 알려진 프로토콜 : 디코드

#패킷처리 단계(New Session)

1. **초기 패킷 처리** : Source 존&주소/유저 ID > PBR/포워딩 조회 > Destination 존 > NAT 정책 평가
2. **사전 보안 정책** : 허용 포트 확인 > 세션 생성(6-tuple : 소스 IP/소스 존/대상 IP/대상 존/대상 포트/프로토콜)
3. **애플리케이션** : 암호화 확인 > 복호화 정책 조회 > 애플리케이션 오버라이드 정책 > App-ID/Content-ID 라벨 지정
4. **보안 정책** : 보안 정책 확인 > 보안 프로파일 확인
5. **사후 정책 처리** : 트래픽 재암호화 > NAT 정책 적용 > 패킷 포워딩

#App-ID 분류 방법

패킷 수신 > 6-Tuple 확인 > 보안 정책 확인 > 알려진 애플리케이션 시그니처 확인 *애플리케이션 식별 작업 >

1. 보안 정책 재확인 > 더이상 디코딩이 필요하지 않은 세션 식별
2. 보안 정책 재확인 > SSH 또는 TLS 암호 해독 *복호화 >애플리케이션 식별 작업
3. 보안 정책 재확인 > 알수없는 프로토콜 : 휴리스틱 적용
4. 보안 정책 재확인 > 알려진 프로토콜 : 디코드

#패킷처리 단계(New Session)

1. **초기 패킷 처리** : Source 존&주소/유저 ID > PBR/포워딩 조회 > Destination 존 > NAT 정책 평가
2. **사전 보안 정책** : 허용 포트 확인 > 세션 생성(6-tuple : 소스 IP/소스 존/대상 IP/대상 존/대상 포트/프로토콜)
3. **애플리케이션** : 암호화 확인 > 복호화 정책 조회 > 애플리케이션 오버라이드 정책 > App-ID/Content-ID 라벨 지정
4. **보안 정책** : 보안 정책 확인 > 보안 프로파일 확인
5. **사후 정책 처리** : 트래픽 재암호화 > NAT 정책 적용 > 패킷 포워딩

#App-ID 분류 방법

패킷 수신 > 6-Tuple 확인 > 보안 정책 확인 > 알려진 애플리케이션 시그니처 확인 *애플리케이션 식별 작업 >

1. 보안 정책 재확인 > 더이상 디코딩이 필요하지 않은 세션 식별
2. 보안 정책 재확인 > SSH 또는 TLS 암호 해독 *복호화 >애플리케이션 식별 작업
3. 보안 정책 재확인 > 알수없는 프로토콜 : 휴리스틱 적용
4. 보안 정책 재확인 > 알려진 프로토콜 : 디코드