ASA HTTP URL 필터 기능과 Regex

목차

소개

이 문서에서는 HTTP 검사 엔진을 사용하는 ASA(Adaptive Security Appliance)에서 URL 필터의 컨피그레이션에 대해 설명합니다.이는 HTTP 요청의 일부가 regex 패턴 목록 사용과 일치할 때 완료됩니다.특정 URL을 차단하거나 일부 URL을 제외한 모든 URL을 차단할 수 있습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

이 섹션에서는 이 문서에 설명된 기능을 구성하는 정보를 제공합니다.

참고:이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용합니다.

구성 단계

다음은 일반적인 컨피그레이션 단계입니다.

1. 차단하거나 허용해야 하는 간단한 도메인 목록 식별
2. 문제의 모든 도메인과 일치하는 regex 클래스 맵을 만듭니다.
3. 이러한 도메인과 일치하는 트래픽을 삭제하거나 허용하는 HTTP 검사 정책 맵 구축
4. 이 HTTP 검사 정책 맵을 모듈형 정책 프레임워크의 HTTP 검사에 적용

일부 도메인을 차단하고 다른 모든 도메인을 허용하거나 모든 도메인을 차단하고 일부만 허용하려고 시도하는지 여부에 관계없이 HTTP 검사 정책 맵을 만드는 경우를 제외하고 단계는 동일합니다.

차단하거나 허용해야 하는 간단한 도메인 목록 식별

이 컨피그레이션 예에서는 이러한 도메인이 차단되거나 허용됩니다.

- cisco1.com
- cisco2.com
- cisco3.com

다음 도메인에 대한 regex 패턴을 구성합니다.

```
regex cisco1.com "cisco1.com"regex cisco2.com "cisco2.com"regex cisco3.com "cisco3.com"
```

문제의 모든 도메인과 일치하는 regex 클래스 맵을 만듭니다.

regex 패턴과 일치하는 regex 클래스를 구성합니다.

```
class-map type regex match-any domain-regex-classmatch regex cisco1.commatch regex
cisco2.commatch regex cisco3.com
```

이러한 도메인과 일치하는 트래픽을 삭제하거나 허용하는 HTTP 검사 정책 맵 구축

이 컨피그레이션의 모양을 이해하려면 이 URL 필터의 목표에 가장 적합한 설명을 선택합니다.위에 작성된 regex 클래스는 허용해야 하는 도메인 목록 또는 차단해야 하는 도메인 목록입니다.

- **나열된 도메인을 제외한 모든 도메인 허용**이 컨피그레이션의 핵심은 나열된 도메인과 일치하는 HTTP 트랜잭션이 "blocked-domain-class"로 분류되는 클래스 맵이 생성되는 것입니다. 이 클래스와 일치하는 HTTP 트랜잭션이 재설정되고 닫힙니다.기본적으로 이러한 도메인과 일치하는 HTTP 트랜잭션만 재설정됩니다.
  ```
  class-map type inspect http match-all blocked-domain-class match request header host regex
  class domain-regex-class!policy-map type inspect http regex-filtering-policy parameters
  class blocked-domain-class  reset log
  ```
- **나열된 도메인을 제외한 모든 도메인 차단**이 컨피그레이션의 핵심은 "match not" 키워드를 사용하여

클래스 맵을 만드는 것입니다. 이렇게 하면 도메인 목록과 일치하지 않는 모든 도메인이 "allowed-domain-class"라는 제목의 클래스와 일치해야 함을 방화벽에 알립니다.해당 클래스와 일치하는 HTTP 트랜잭션이 재설정되고 닫힙니다.기본적으로 모든 HTTP 트랜잭션은 나열된 도메인과 일치하지 않는 한 재설정됩니다.

```
class-map type inspect http match-all allowed-domain-class match not request header host
regex class domain-regex-class!policy-map type inspect http regex-filtering-policy
parameters class allowed-domain-class  reset log
```

이 HTTP 검사 정책 맵을 모듈형 정책 프레임워크의 HTTP 검사에 적용

HTTP 검사 정책 맵이 "regex-filtering-policy"로 구성되었으므로, 이 정책 맵을 존재하는 HTTP 검사 또는 Modular Policy Framework의 새 검사에 적용합니다.예를 들어 "global_policy"에 구성된 "inspection_default" 클래스에 검사가 추가됩니다.

```
policy-map global_policy class inspection_default  inspect http regex-filtering-policy
```

일반적인 문제

HTTP 검사 정책 맵 및 HTTP 클래스 맵이 구성된 경우 원하는 목표에 맞게 일치 또는 매치가 구성되지 않았는지 확인합니다.이 키워드는 건너뛰고 의도하지 않은 동작을 발생시키는 간단한 키워드입니다.또한 모든 고급 패킷 처리와 마찬가지로 이러한 형식의 regex 프로세싱으로 인해 ASA CPU 사용률이 증가하고 처리량이 감소할 수 있습니다.regex 패턴이 점점 더 추가될 때 주의하십시오.