보안 ASA 방화벽 사용 설명서

목차

소개

이 문서에서는 네트워크의 전반적인 보안을 강화하는 Cisco ASA 장치를 보호하는 데 도움이 되는 정보에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ASA(Active Security Appliance) 9.16(1) 이상

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

배경 정보

이 문서는 4개의 섹션으로 구성되어 있습니다.

1. 관리 플레인 강화 - SNMP, SSH 등의 모든 ASA 관련 관리/ToBox 트래픽에 적용됩니다.
2. Securing config - 실행 중인 컨피그레이션 등에 대해 비밀번호 입력 등을 중지할 수 있는 명령입니다.
3. 로깅 및 모니터링 - ASA에서의 로깅과 관련된 모든 설정에 적용됩니다.

4. 통과 트래픽 - ASA를 통과하는 트래픽에 적용됩니다.

이 문서에 포함된 보안 기능 범위에서는 기능을 구성하는 데 충분한 세부 정보를 제공하는 경우가 많습니다. 그러나 그렇지 못한 경우 기능에 각별히 주의를 기울여야 하는지 사용자가 평가할 수 있도록 기능이 설명되어 있습니다. 가능하고 적절한 경우 이 문서에는 구현되면 네트워크를 보호하는 데 도움이 되는 권장 사항이 포함되어 있습니다.

관련 제품

이 컨피그레이션은 Cisco ASA Software Version 9.1x에서도 사용할 수 있습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

보안 운영

보안 네트워크 운영은 중요한 주제입니다. 이 문서의 대부분은 Cisco ASA 디바이스의 보안 컨피그레이션에 대해 다루고 있지만 컨피그레이션만으로는 네트워크를 완전히 보호하는 것은 아닙니다. 네트워크에서 사용 중인 운영 절차가 기본 디바이스 컨피그레이션에 못지 않게 보안에 중요합니다.

이러한 주제에는 구현 시 권고하는 운영 권장 사항이 포함되어 있습니다. 이러한 주제에서는 중요한 특정 네트워크 운영 영역을 강조하여 설명하지만 포괄적이지는 않습니다.

Cisco 보안 권고 및 대응 모니터링

Cisco PSIRT(Product Security Incident Response Team)에서는 Cisco 제품의 보안 관련 문제에 관한 간행물을 작성하고 유지관리합니다. 이 간행물은 일반적으로 PSIRT Advisories라고 합니다. 덜 심각한 문제의 커뮤니케이션에 사용되는 방법이 Cisco Security Response입니다. 보안 권고 및 응답은 PSIRT에서 확인할 수 있습니다.

이 커뮤니케이션 수단에 대한 자세한 정보는 Cisco 보안 취약점 정책에서 찾아볼 수 있습니다.

보안 네트워크를 유지 보수하려면 공개된 Cisco 보안 권고 및 대응을 알아야 합니다. 취약점에 대한 지식이 있어야 네트워크에 발생할 수 있는 위협을 평가할 수 있습니다. 이 평가 프로세스에 대한 도움은 보안 취약성 공지에 대한 위험 분류를 참조하십시오.

인증, 권한 부여 및 계정 관리(AAA) 활용

AAA(Authentication, Authorization, and Accounting) 프레임워크는 네트워크 디바이스 보안에 중요합니다. AAA 프레임워크는 관리 세션에 대한 인증을 제공하며, 사용자가 특정 관리자 정의 명령어만 사용하도록 제한하고, 모든 사용자가 입력한 모든 명령어를 기록할 수도 있습니다. AAA 활용 방법에 대한 자세한 내용은 이 문서의 인증, 권한 부여 및 계정 관리 섹션을 참조하십시오.

로그 수집 및 모니터링 중앙 집중화

보안 사고와 관련된 기존 이벤트, 새로운 이벤트 및 이력 이벤트에 대한 지식을 얻으려면 조직에 이

벤트 로깅 및 상관관계에 관한 통합 전략이 있어야 합니다. 이 전략에서는 모든 네트워크 디바이스의 로깅을 활용하고 사전 패키지된 맞춤형 상관관계 기능을 사용해야 합니다.

중앙 집중식 로깅을 구현한 후에는 분석과 사고 추적을 기록하는 구조화된 접근 방식을 개발해야 합니다. 조직의 요구 사항에 따라 이 접근 방식은 간단한 로그 데이터 검토부터 고급 규칙 기반 분석까지 다양합니다.

가능한 경우 보안 프로토콜 사용

민감한 네트워크 관리 데이터를 전달하기 위해 수많은 프로토콜이 사용됩니다. 가능한 경우 항상 보안 프로토콜을 사용해야 합니다. 인증 데이터와 관리 정보를 모두 암호화하기 위해 텔넷 대신 SSH를 사용하도록 보안 프로토콜을 선택할 수 있습니다. 또한 컨피그레이션 데이터를 복사할 때 보안 파일 전송 프로토콜을 사용해야 합니다. 예를 들어, FTP 또는 TFTP 대신 SCP(Secure Copy Protocol)를 사용합니다.

NetFlow로 트래픽 가시성 확보

NetFlow를 사용하면 네트워크의 트래픽 흐름을 모니터링할 수 있습니다. 원래 네트워크 관리 애플리케이션에 트래픽 정보를 내보내는 데 사용하는 NetFlow는 라우터에 플로우 정보를 표시하는 데도 사용할 수 있습니다. 이 기능을 사용하면 어떤 트래픽이 실시간으로 네트워크를 이동하는지 볼 수 있습니다. 플로우 정보를 원격 컬렉터에 내보내는지 여부에 상관없이, 필요한 경우 사후 대응식으로 사용할 수 있도록 NetFlow에 대해 네트워크 디바이스를 구성하는 것이 좋습니다.

컨피그레이션 관리

컨피그레이션 관리는 컨피그레이션 변경을 제안, 검토, 승인 및 구축하는 프로세스입니다. Cisco ASA 디바이스 컨피그레이션의 경우 컨피그레이션 아카이브와 보안이라는 두 가지 추가 컨피그레이션 관리 측면이 중요합니다.

컨피그레이션 아카이브를 사용하여 네트워크 디바이스의 변경 사항을 롤백할 수 있습니다. 보안 상황에서, 변경된 보안 사항과 변경 시기를 판별하기 위해 컨피그레이션 아카이브를 사용할 수도 있습니다. AAA 로그 데이터와 함께 이 정보를 사용하면 네트워크 디바이스의 보안 감사에 도움이 될 수 있습니다.

Cisco ASA 디바이스의 컨피그레이션에는 여러 가지 중요한 세부 정보가 포함되어 있습니다. 사용자 이름, 비밀번호 및 액세스 제어 목록의 콘텐츠는 이 정보 유형의 예입니다. Cisco ASA 디바이스 컨피그레이션을 아카이브하기 위해 사용하는 리포지토리는 보호되어야 합니다. 이 정보에 대한 액세스가 안전하지 않으면 전체 네트워크의 보안이 저해될 수 있습니다.

관리 플레인

관리 플레인은 네트워크의 관리 목표를 달성하는 기능으로 구성됩니다. 이 기능에는 SNMP 또는 NetFlow를 사용한 통계 수집 외에도 SSH를 사용하는 인터랙티브 관리 세션이 포함됩니다. 네트워크 디바이스의 보안을 고려할 때 관리 플레인을 보호하는 것이 중요합니다. 보안 사고로 인해 관리 플레인의 기능이 저하될 수 있는 경우 네트워크를 복구하거나 안정화할 수 없습니다.

관리 플레인 강화

관리 플레인은 디바이스가 구축된 네트워크와 해당 운영을 모니터링할 뿐만 아니라 디바이스에 액세스하고 디바이스를 구성 및 관리하는 데 사용됩니다. 관리 플레인은 이러한 기능의 운영을 위해 트래픽을 수신하고 전송하는 플레인입니다. 관리 플레인에서 사용하는 프로토콜 목록은 다음과 같습니다.

- Simple Network Management Protocol
- SSH(Secure Shell) 프로토콜
- FTP(File Transfer Protocol)
- TFTP(Trivial File Transfer Protocol)
- SCP(Secure Copy) 프로토콜
- TACACS+
- RADIUS
- Netflow
- Network Time Protocol(네트워크 타이밍 프로토콜)
- Syslog
- ICMP
- SMB

참고: 일반 텍스트이므로 텔넷을 활성화하지 않는 것이 좋습니다.

비밀번호 관리

비밀번호는 리소스 또는 디바이스에 대한 액세스를 제어합니다. 이 작업은 요청을 인증하기 위해 사용하는 비밀번호 또는 암호를 정의하여 수행합니다. 리소스 또는 디바이스에 대한 액세스 요청을 수신하면 비밀번호와 ID를 확인하기 위해 요청을 검사하고, 결과에 따라 액세스 권한을 부여, 거부 또는 제한할 수 있습니다. 모범 사례에 따라 비밀번호는 TACACS+ 또는 RADIUS 인증 서버로 관리되어야 합니다. 그러나 TACACS+ 또는 RADIUS 서비스가 실패하는 경우에는 권한 부여된 액세스를 위해 로컬에서 구성된 비밀번호가 여전히 필요합니다. 디바이스에는 NTP 키, SNMP 커뮤니티 문자열 또는 라우팅 프로토콜 키와 같이 컨피그레이션에 있는 기타 비밀번호 정보도 있을 수 있습니다.

ASA 9.7(1)에서는 로컬 비밀번호에 PBKDF2 해싱을 도입했습니다. 로컬 사용자 이름 및 모든 길이의 enable 비밀번호는 PBKDF2(Password-Based Key Derivation Function 2) 해시를 사용하여 컨피그레이션에 저장됩니다. 이전에는 32자 이하의 비밀번호가 MD5 기반 해싱 방법을 사용했습니다. 기존 비밀번호는 새 비밀번호를 입력하지 않는 한 MD5 기반 해시를 계속 사용합니다. 다운그레이드 지침은 일반 작업 컨피그레이션 가이드의 소프트웨어 및 컨피그레이션 장을 참조하십시오.

HTTP 서비스 활성화

ASDM을 사용하려면 HTTPS 서버를 활성화하고 ASA에 대한 HTTPS 연결을 허용해야 합니다. 보안 어플라이언스는 사용 가능한 경우 컨텍스트당 최대 5개의 동시 ASDM 인스턴스를 허용하며, 모든 컨텍스트 간에 최대 32개의 ASDM 인스턴스를 허용합니다. ASDM 액세스 사용을 구성하려면

```
http server enable <port>
```

ACL 목록에 필요한 IP만 허용합니다. 광범위한 접근을 허용하는 것은 좋은 방법이 아니다.

```
http 0.0.0.0 0.0.0.0 <interface>
```

ASDM 액세스 제어 구성:

```
http <remote_ip_address> <remote_subnet_mask> <interface_name>
```

```
// Set server version
ASA(config)# ssl server-version tlsv1 tlsv1.1 tlsv.1.2

// Set client version
ASA(config) # ssl client-version tlsv1 tlsv1.1 tlsv.1.2
```

ASA에는 기본적으로 표시된 순서대로 이러한 암호가 활성화되어 있습니다.

```
ciscoasa(config)# ssl cipher ?

configure mode commands/options:
  default   Specify the set of ciphers for outbound connections
  dtlsv1    Specify the ciphers for DTLSv1 inbound connections
  dtlsv1.2  Specify the ciphers for DTLSv1.2 inbound connections
  tlsv1     Specify the ciphers for TLSv1 inbound connections
  tlsv1.1   Specify the ciphers for TLSv1.1 inbound connections
  tlsv1.2   Specify the ciphers for TLSv1.2 inbound connections
ciscoasa(config)# ssl cipher dtlsv1 ?

configure mode commands/options:
  all     Specify all ciphers
  low     Specify low strength and higher ciphers
  medium  Specify medium strength and higher ciphers
  fips    Specify only FIPS-compliant ciphers
  high    Specify only high-strength ciphers
  custom  Choose a custom cipher configuration string.
```

기본값이 높습니다.

- all 키워드는 모든 암호를 사용하도록 지정합니다. hmac-sha1 hmac-sha1-96 hmac-sha2-256 hmac-md5 hmac-md5-96

- custom 키워드는 사용자 지정 암호 암호화 컨피그레이션 문자열을 콜론으로 구분하여 지정합니다.
- fips 키워드는 FIPS 호환 암호만 지정합니다. hmac-sha1 hmac-sha2-256
- high 키워드는 고강도 암호(기본값)만 지정합니다. hmac-sha2-256
- low 키워드는 low, medium, high strength 암호를 지정합니다. hmac-sha1 hmac-sha1-96 hmac-md5 hmac-md5-96 hmac-sha2-256
- medium 키워드는 중급 및 고강도 암호 hmac-sha1 hmac-sha1-96 hmac-sha2-256을 지정합니다

ASA는 기본적으로 임시 자체 서명 인증서를 사용하며, 이는 재부팅할 때마다 변경됩니다. 단일 인증서를 찾는 경우 이 링크를 사용하여 영구 자체 서명 인증서를 생성할 수 있습니다.

ASA는 ASDM, 클라이언트리스 SSVPN 및 AnyConnect VPN에 대한 보안 메시지 전송을 위해 TLS 버전 1.2를 지원합니다. 이러한 명령이 도입되었거나 수정된 명령: ssl client-version, ssl server-version, ssl cipher, ssl trust-point, ssl dh-group, show ssl, show ssl cipher, show vpn-sessiondb.

```
ASA-1/act(config)# ssl server-version ?

configure mode commands/options:
  tlsv1    Enter this keyword to accept SSLv2 ClientHellos and negotiate TLSv1
           (or greater)
  tlsv1.1  Enter this keyword to accept SSLv2 ClientHellos and negotiate
           TLSv1.1 (or greater)
  tlsv1.2  Enter this keyword to accept SSLv2 ClientHellos and negotiate
           TLSv1.2 (or greater)
```

```
ASA-1/act(config)# ssl cipher ?

configure mode commands/options:
  default  Specify the set of ciphers for outbound connections
  dtlsv1   Specify the ciphers for DTLSv1 inbound connections
  tlsv1    Specify the ciphers for TLSv1 inbound connections
  tlsv1.1  Specify the ciphers for TLSv1.1 inbound connections
  tlsv1.2  Specify the ciphers for TLSv1.2 inbound connections
```

SSH 사용

ASA는 관리를 위해 ASA에 대한 SSH 연결을 허용합니다. ASA에서는 컨텍스트당 최대 5개의 동시 SSH 연결을 허용합니다(사용 가능한 경우). 모든 컨텍스트에서 최대 100개의 연결을 분할할 수 있습니다.

```
hostname <device_hostname>
domain-name <domain-name>
crypto key generate rsa modulus 2048
```

기본 키 쌍 유형은 general key입니다. 기본 모듈러스 크기는 1024입니다. 키 쌍을 저장하기 위한 NVRAM 공간의 양은 ASA 플랫폼에 따라 다릅니다. 30개 이상의 키 쌍을 생성하는 경우 한도에 도달할 수 있습니다.

표시된 유형(rsa 또는 dsa)의 키 쌍을 제거하려면

```
crypto key zeroize { rsa | eddsa | ecdsa } [ label key-pair-label ] [ default ] [ noconfirm ]
```

원격 디바이스 액세스를 위한 SSH를 구성합니다.

```
ssh <remote_ip_address> <remote_subnet_mask> <interface_name>
```

DH(Diffie-Hellman) 그룹 1, DH 그룹 14 또는 Curve25519 키 교환 방법을 사용하여 키를 교환하려면 글로벌 컨피그레이션 모드에서 ssh key-exchange 명령을 사용합니다. 9.1(2)부터 ASA는 SSH에 dh-group14-sha1을 지원합니다.

```
ASA(config)#ssh key-exchange group dh-group14-sha256
```

로그인 세션에 대한 시간 초과 구성

```
// Configure Console timeout
ASA(config)#console timeout 10

// Configure Console timeout
ASA(config)#ssh timeout 10
```

비밀번호 관리

비밀번호는 리소스 또는 디바이스에 대한 액세스를 제어합니다. 이 작업은 요청을 인증하기 위해 사용하는 비밀번호 또는 암호를 정의하여 수행합니다. 리소스 또는 디바이스에 대한 액세스 요청을 수신하면 비밀번호와 ID를 확인하기 위해 요청을 검사하고, 결과에 따라 액세스 권한을 부여, 거부 또는 제한할 수 있습니다. 모범 사례에 따라 비밀번호는 TACACS+ 또는 RADIUS 인증 서버로 관리

되어야 합니다. 그러나 TACACS+ 또는 RADIUS 서비스가 실패하는 경우에는 권한 부여된 액세스를 위해 로컬에서 구성된 비밀번호가 여전히 필요합니다. 디바이스에는 NTP 키, SNMP 커뮤니티 문자열 또는 라우팅 프로토콜 키와 같이 컨피그레이션에 있는 기타 비밀번호 정보도 있을 수 있습니다.

로컬 사용자 및 암호화된 비밀번호 구성

```
username <local_username> password <local_password> encrypted
```

Enable 비밀번호 구성

```
enable password <enable_password> encrypted
```

활성화 모드에 대한 AAA 인증 구성

```
ASA(config)#aaa authentication enable console LOCAL
```

인증, 권한 부여 및 계정 관리(AAA)

AAA(Authentication, Authorization, and Accounting) 프레임워크는 네트워크 디바이스에 대한 인터랙티브 액세스 보안에 중요합니다. AAA 프레임워크에서는 네트워크 요구 사항에 따라 조정할 수 있는 구성하기 쉬운 환경을 제공합니다.

TACACS+ 인증

TACACS+는 ASA가 원격 AAA 서버에 대한 관리 사용자 인증에 사용할 수 있는 인증 프로토콜입니다. 이러한 관리 사용자는 SSH, HTTPS, 텔넷 또는 HTTP를 통해 ASA 디바이스에 액세스할 수 있습니다.

TACACS+ 인증 또는 더욱 일반적으로 AAA 인증에서는 각 네트워크 관리자가 개별 사용자 계정을 사용하는 기능을 제공합니다. 단일 공유 비밀번호에 의존하지 않는 경우 네트워크 보안이 향상되므로 사용자의 책임이 강화됩니다.

RADIUS는 TACACS+와 용도가 유사한 프로토콜이지만 네트워크를 통해 전송된 비밀번호만 암호화합니다. 반면, TACACS+는 사용자 이름과 비밀번호를 모두 포함하는 전체 TCP 페이로드를 암호화합니다. 따라서 AAA 서버에서 TACACS+를 지원하는 경우 RADIUS에 우선하여 TACACS+를 사용할 수 있습니다. 이러한 두 가지 프로토콜의 자세한 비교는 TACACS+ 및 RADIUS 비교를 참조하십시오.

TACACS+ 인증은 다음 예와 유사한 컨피그레이션으로 Cisco ASA 디바이스에서 활성화할 수 있습니다.

```
aaa authentication serial console Tacacs
aaa authentication ssh console Tacacs
aaa authentication http console Tacacs
aaa authentication telnet console Tacacs
```

ASA 이미지 서명 및 확인

소프트웨어 버전 9.3.1부터 이제 ASA 이미지가 디지털 서명을 사용하여 서명됩니다. ASA가 부팅된 후 디지털 서명이 확인됩니다.

```
ASA-1/act(config)# verify flash:/asa941-smp-k8.bin
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Embedded Hash SHA-512: 0e707a0e45b1c7c5afa9ef4e802a273677a5e46f7e1d186292abe1154
Computed Hash SHA-512: 0e707a0e45b1c7c5afa9ef4e802a273677a5e46f7e1d186292abe1154
CCO Hash      SHA-512: 1b6d41e893868aab9e06e78a9902b925227c82d8e31978ff2c412c18a
Signature Verified


ASA(config)# verify /signature running
Requesting verify signature of the running image...

Starting image verification
Hash Computation:    100% Done!
Computed Hash   SHA2: 2fbb0f62b5fbc61b081acfca76bddbb2
                      26ce7a5fb4b424e5e21636c6c8a7d665
                      1e688834203dfb7ffa6eaefc7fdf9d3d
                      1d0a063a20539baba72c2526ca37771c


Get key records from key storage: PrimaryASA, key_store_type: 6
Embedded Hash   SHA2: 2fbb0f62b5fbc61b081acfca76bddbb2
                      26ce7a5fb4b424e5e21636c6c8a7d665
                      1e688834203dfb7ffa6eaefc7fdf9d3d
                      1d0a063a20539baba72c2526ca37771c

Returned. rc: 0, status: 1
The digital signature of the running image verified successfully

ASA-1/act(config)# show software authenticity running
Image type : Release
 Signer Information
 Common Name : abraxas
 Organization Unit : ASAv
 Organization Name : CiscoSystems
 Certificate Serial Number : 550DBBD5
 Hash Algorithm : SHA2 512
 Signature Algorithm : 2048-bit RSA
 Key Version : A
```

클럭 시간대 구성

```
clock timezone GMT <hours offset>
```

NTP 구성

NTP(Network Time Protocol)가 특별히 위험한 서비스는 아니지만, 불필요한 모든 서비스는 공격 벡터를 나타낼 수 있습니다. NTP를 사용하는 경우 신뢰할 수 있는 시간 소스를 명시적으로 구성하고 적절한 인증을 사용하는 것이 중요합니다. 인증서에 의존하여 1단계 인증을 수행할 때 성공적으로 VPN을 연결하는 용도 외에 syslog 용도(예: 잠재적 공격의 포렌식 검사 중)로도 정확하고 신뢰할 수 있는 시간이 필요합니다.

- NTP 시간대 - NTP를 구성할 때 타임스탬프가 정확하게 상관관계를 보여줄 수 있도록 시간대를 구성해야 합니다. 전역적으로 존재하는 네트워크에서 디바이스의 시간대를 구성하는 방법은 일반적으로 두 가지가 있습니다. 한 가지 방법은 이전에는 GMT(Greenwich Mean Time)라고 한 UTC(Coordinated Universal Time)로 모든 네트워크 디바이스를 구성하는 것입니다. 다른 방법은 로컬 표준 시간대를 사용하여 네트워크 장치를 구성하는 것입니다. ntp server ip_address [key key_id] [source interface_name] [prefer]
- NTP 인증 - NTP 인증을 구성하면 신뢰할 수 있는 NTP 피어 간에 NTP 메시지를 확실히 교환할 수 있습니다. Enable authentication using the ntp authenticate 명령을 사용하여 이 서버에 대해 신뢰할 수 있는 키 ID를 설정합니다. 인증을 활성화하면 ASA는 패킷에서 올바른 신뢰 키를 사용하는 경우에만 NTP 서버와 통신합니다. NTP 서버와의 인증을 활성화하려면 글로벌 컨피그레이션 모드에서 ntp authenticate 명령을 사용합니다.

```
ASA(config)#ntp authenticate
```

DHCP 서버 서비스(사용되지 않는 경우)

```
clear configure dhcpd
no dhcpd enable <interface_name>
```

참고: ASA는 CDP를 지원하지 않습니다.

컨트롤 플레인 액세스 목록

to-the-box 관리 트래픽에 대한 액세스 제어 규칙(http, ssh 또는 telnet과 같은 명령으로 정의됨)은 control-plane 옵션으로 적용되는 액세스 목록보다 우선순위가 높습니다. 따라서 이렇게 허용된 관

리 트래픽은 to-the-box 액세스 목록에 의해 명시적으로 거부된 경우에도 허용될 수 있습니다.

```
access-list <name> in interface <Interface_name> control-plane
```

ASA에서

다음은 ASA에 파일을 복사/전송하는 데 사용할 수 있는 프로토콜입니다.

일반 텍스트:

- FTP
- HTTP
- TFTP
- SMB

보안:

- HTTPS
- SCP(Secure Copy Client) ASA는 SCP 클라이언트에서 SCP 서버로 또는 SCP 서버로부터 파일을 전송하도록 지원합니다.

통과 트래픽용

TCP 시퀀스 번호 임의 설정

각 TCP 연결에는 두 개의 ISN이 있습니다. 하나는 클라이언트에서 생성하고 다른 하나는 서버에서 생성합니다. ASA는 인바운드 방향과 아웃바운드 방향 모두를 통과하는 TCP SYN의 ISN을 임의로 지정합니다.

보호된 호스트의 ISN을 임의로 설정하면 공격자가 새 연결에 대한 다음 ISN을 예측하거나 새 세션을 가로챌 수 있습니다.

필요한 경우 TCP 초기 시퀀스 번호 임의 설정을 비활성화할 수 있습니다. 예를 들면 다음과 같습니다.

- 다른 인라인 방화벽도 초기 시퀀스 번호를 임의로 지정하는 경우, 트래픽에 영향을 미치지 않더라도 두 방화벽이 모두 이 작업을 수행할 필요는 없습니다.
- ASA를 통해 eBGP 멀티 홉을 사용하는 경우 eBGP 피어가 MD5를 사용합니다. 임의 설정은 MD5 체크섬을 중단합니다.
- ASA가 연결의 시퀀스 번호를 임의로 설정하지 않도록 요구하는 WAAS 장치를 사용하는 경우 .

TTL 감소

기본적으로 는 Traceroute를 수행할 때 ASA가 라우터 홉으로 표시되지 않기 때문에 IP 헤더의 TTL을 감소시키지 않습니다.

dnsguard

쿼리당 하나의 DNS 응답을 적용합니다. 전역 컨피그레이션 모드에서 명령을 사용하여 활성화할 수 있습니다.

```
ASA(config)#dns-guard
```

프래그먼트 체인 프래그먼트화 확인 구성

패킷 조각화를 추가로 관리하고 NFS와의 호환성을 향상시키려면 글로벌 컨피그레이션 모드에서 fragment 명령을 사용합니다.

```
fragment reassembly { full | virtual } { size | chain | timeout limit } [ interface ]
```

프로토콜 검사 구성

검사 엔진은 사용자 데이터 패킷에 IP 주소 지정 정보를 포함하거나 동적으로 할당된 포트에서 보조 채널을 여는 서비스에 필요합니다. 이러한 프로토콜을 사용하려면 ASA에서 패킷을 빠른 경로로 전달하는 대신 심층 패킷 검사를 수행해야 합니다. 따라서 검사 엔진은 전체 처리량에 영향을 미칠 수 있습니다. 애플리케이션 레이어 프로토콜 검사에 대한 자세한 내용은 ASA 9.4 컨피그레이션 가이드를 참조하십시오.

ASA에 대한 검사는 이 명령을 사용하여 활성화할 수 있습니다.

```
policy-map <Policy-map_name>
 class inspection_default
  inspect <Protocol>

service-policy <Policy-map_name> interface <Interface_name> (Per Interface)
service-policy <Policy-map_name> global (Globally)
```

기본적으로 ASA는 global_policy가 전역적으로 활성화되어 있습니다.

유니캐스트 역방향 경로 전달 구성

```
ip verify reverse-path interface <interface_name>
```

RPF 검사로 인해 트래픽이 삭제되면 ASA 증분의 asp 삭제 카운터가 표시됩니다.

<#root>

```
ASA(config)# show asp drop

Frame drop:
  Invalid TCP Length (invalid-tcp-hdr-length)                    21
  Reverse-path verify failed (rpf-violated)                      90


// Check Reverse path statistics

ASA(config)# sh ip verify statistics
interface inside: 11 unicast rpf drops


interface outside: 79 unicast rpf drops
```

위협 탐지

위협 탐지는 방화벽 관리자가 내부 네트워크 인프라에 도달하기 전에 공격을 식별, 이해, 차단하는 데 필요한 툴을 제공합니다. 이를 위해 이 기능은 여러 가지 다양한 트리거 및 통계에 의존하며, 이 내용은 이 섹션에서 자세히 설명합니다.

ASA에서의 위협 탐지에 대한 자세한 설명은 ASA 위협 탐지 기능 및 컨피그레이션을 참조하십시오 .

봇넷 필터

BotNet 트래픽 필터는 내부 DNS 클라이언트와 외부 DNS 서버 간의 DNS(Domain Name Server) 요청 및 응답을 모니터링합니다. DNS 응답이 처리되면 응답과 연결된 도메인이 알려진 악성 도메인의 데이터베이스를 기준으로 점검됩니다. 일치하는 항목이 있는 경우 DNS 응답에 있는 IP 주소에 대한 추가 트래픽은 차단됩니다.

악성코드는 알 수 없는 호스트에 설치되는 악성 소프트웨어입니다. 개인 데이터(비밀번호, 신용카드 번호, 키 스트로크 또는 독점 데이터) 전송과 같은 네트워크 활동을 시도하는 악성코드는 악성코드가 알려진 악성 IP 주소에 대한 연결을 시작할 때 Botnet Traffic Filter에서 탐지될 수 있습니다.

Botnet Traffic Filter는 알려진 악성 도메인 이름 및 IP 주소의 동적 데이터베이스(차단된 목록)를 기준으로 수신 및 발신 연결을 확인한 다음 의심스러운 활동을 로깅하거나 차단합니다.

선택한 차단 목록 주소로 Cisco 동적 데이터베이스를 보완하려면 해당 주소를 고정 차단 목록에 추가합니다. 동적 데이터베이스에 차단 목록에 포함될 수 없다고 생각하는 차단 목록 주소가 포함되어 있는 경우, 이를 고정 허용 목록에 수동으로 입력할 수 있습니다. 허용되는 목록 주소는 여전히 syslog 메시지를 생성하지만 차단된 목록 syslog 메시지만 대상으로 하므로 정보를 제공합니다. 자세한 내용은 봇넷 트래픽 필터 구성을 참조하십시오.

연결되지 않은 서브넷에 대한 ARP 캐시 추가

기본적으로 ASA는 직접 연결되지 않은 서브넷 IP 주소에 대해 ARP에 응답하지 않습니다. ASA 인터페이스의 동일한 서브넷 IP에 속하지 않는 ASA의 NAT IP가 있는 경우 NATted IP에 대해 프록시-ARP에 대해 ASA의 arp permit-nonconnected를 활성화해야 할 수 있습니다.

```
arp permit-nonconnected
```

항상 이전 명령을 활성화하지 않고 NAT가 작동하도록 업스트림 및 다운스트림 디바이스에서 올바른 라우팅을 사용하는 것이 좋습니다.

로깅 및 모니터링

SNMP 구성

이 섹션에서는 ASA 디바이스 내에서 SNMP 구축을 보호하기 위해 사용할 수 있는 몇 가지 방법을 중점적으로 설명합니다. 네트워크 데이터와 이 데이터를 전송할 네트워크 디바이스 모두의 기밀성, 무결성 및 가용성을 보호하려면 SNMP의 보안을 적절하게 설정하는 것이 중요합니다. SNMP에서는 네트워크 디바이스의 상태에 대한 풍부한 정보를 제공합니다. 이 정보는 네트워크에 대한 공격을 수행하기 위해 이 데이터를 활용하려는 악의적인 사용자로부터 보호될 수 있습니다.

SNMP 커뮤니티 문자열

커뮤니티 문자열은 디바이스의 SNMP 데이터에 대한 액세스(읽기 전용 및 읽기-쓰기 액세스 모두)를 제한하기 위해 ASA 디바이스에 적용되는 비밀번호입니다. 모든 비밀번호와 마찬가지로 이러한 커뮤니티 문자열을 사소한 것이 아님을 확인하기 위해 신중하게 선택할 수 있습니다. 커뮤니티 문자열은 네트워크 보안 정책에 따라 정기적으로 변경될 수 있습니다. 예를 들어 네트워크 관리자가 역할을 변경하거나 회사를 떠날 때 문자열을 변경할 수 있습니다.

SNMP 읽기 액세스 사용

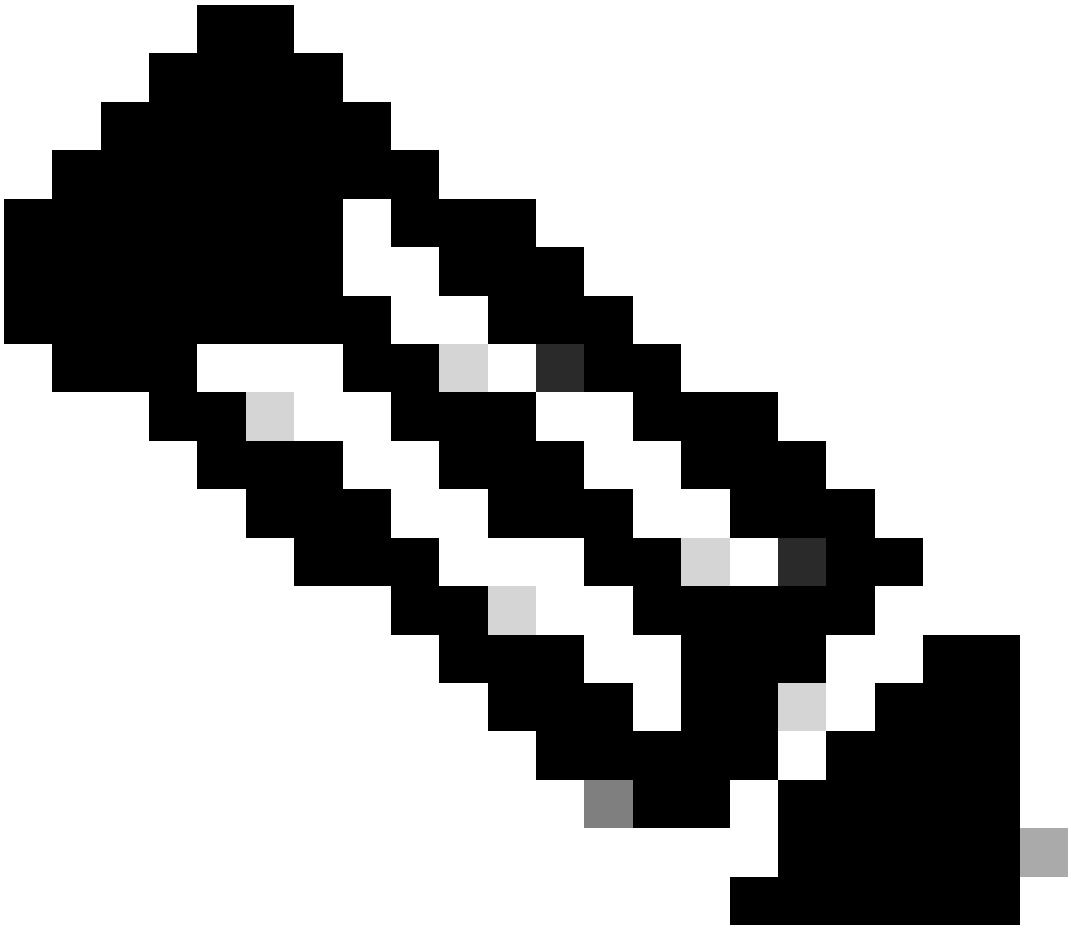
```
snmp-server host <interface_name> <remote_ip_address>
```

SNMP 트랩 사용

```
snmp-server enable traps all
```

Syslog 구성

원격 syslog 서버에 로깅 정보를 전송하는 것이 좋습니다. 그러면 네트워크 디바이스 전체에서 네트워크와 보안 이벤트의 상관성을 더욱 효율적으로 분석하고 이들을 감사할 수 있습니다.



참고: Syslog 메시지는 UDP와 일반 텍스트로 불안정하게 전송됩니다.

따라서 syslog 트래픽을 포함하도록 네트워크에서 관리 트래픽(예: 암호화 또는 대역외 액세스)에 제공하는 모든 보호를 확장할 수 있습니다. ASA에서 이 대상으로 로그를 전송하도록 구성할 수 있

습니다.

- ASDM
- 버퍼
- 플래시
- Email
- FTP 서버
- 트랩으로서의 SNMP 서버
- Syslogs 서버

콘솔 로깅 심각도 수준 구성

```
logging console critical
```

TCP 기반 syslog도 사용할 수 있습니다. 모든 syslog는 일반 텍스트 또는 TCP의 경우 암호화된 형식으로 syslog 서버에 전송할 수 있습니다.

평문

logging host interface_name syslog_ip [tcp/ 포트

암호화

logging host interface_name syslog_ip [tcp/ 포트 | [보안]

TCP 연결을 syslogs 서버와 설정할 수 없는 경우 모든 새 연결을 거부할 수 있습니다. logging permit-hostdown 명령을 입력하여 이 기본 동작을 변경할 수 있습니다.

로그 메시지의 타임스탬프 구성

로깅 타임스탬프 컨피그레이션은 네트워크 디바이스 전체의 이벤트 상관관계를 지정하는 데 도움이 됩니다. 로깅 데이터 상관관계를 지정할 수 있으려면 정확하고 일관된 로깅 타임스탬프 컨피그레이션을 구현해야 합니다.

```
logging timestamp
```

syslog와 관련된 추가 정보는 ASA Syslog 컨피그레이션 예를 참조하십시오.

Netflow 구성

특히 사고 대응 중이나 네트워크 성능이 저조한 동안 네트워크 트래픽을 신속하게 식별하여 역추적해야 하는 경우도 있습니다. NetFlow에서는 네트워크의 모든 트래픽을 표시할 수 있습니다. 또한 장기간의 트렌드와 자동 분석을 제공할 수 있는 컬렉터와 함께 NetFlow를 구현할 수 있습니다.

Cisco ASA는 NetFlow 버전 9 서비스를 지원합니다. NSEL의 ASA 및 ASASM 구현에서는 플로우에서 중요한 이벤트를 나타내는 레코드만 내보내는 스테이트풀 IP 플로우 추적 방법을 제공합니다. 스테이트풀 플로우 추적에서는 추적된 플로우가 일련의 상태 변경을 거칩니다. NSEL 이벤트는 흐름 상태에 대한 데이터를 내보내는 데 사용되며 상태 변경을 일으킨 이벤트에 의해 트리거됩니다.

ASA의 Netflow에 대한 자세한 내용은 Cisco ASA NetFlow 구현 가이드를 참조하십시오.

구성 보안

컨피그레이션의 비밀번호

모든 비밀번호와 키는 암호화되거나 난독화되어 있습니다. show running-config는 실제 비밀번호를 표시하지 않습니다.

이러한 백업은 ASA에서 백업/복원에 사용할 수 없습니다. 복원 목적으로 수행되는 백업은 more system:running-config 명령을 사용하여 수행됩니다. ASA 컨피그레이션 비밀번호는 기본 암호를 사용하여 암호화할 수 있습니다. 자세한 내용은 비밀번호 암호화를 참조하십시오.

서비스 비밀번호 복구

이를 비활성화하면 비밀번호 복구 메커니즘을 비활성화하고 ROMMON에 대한 액세스를 비활성화할 수 있습니다. ROMMON이 컨피그레이션 파일 및 이미지를 포함한 모든 파일 시스템을 지우는 방법만이 분실 또는 분실 비밀번호로부터 복구할 수 있습니다. 컨피그레이션을 백업하고 ROMMON 명령줄에서 이미지를 복원하는 메커니즘을 가질 수 있습니다.

문제 해결

사용 가능한 문제 해결 정보가 없습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.