01 용어 정리

용어 정리

VoIP 가이드는 인터넷 전화 트래픽을 게이트웨이가 안전하게 통과시키는 방법을 다룹니다. 이 가이드를 읽는 데 바탕이 되는 핵심 용어를 흐름에 따라 풀어 둡니다.

VoIP의 기본

VoIP(Voice over IP) 는 음성 통화를 IP 네트워크로 주고받는 기술입니다. 통화는 두 종류의 신호로 이뤄집니다 — **Media(미디어)** 는 실제 음성 대화 스트림, **Control/Signaling(제어·시그널링)** 은 다이얼 톤·벨소리처럼 통화를 만들고 끊는 제어 입니다(기술과 표준).

VoIP는 복잡한 프로토콜이 여러 포트를 통해 위협 정보를 나를 수 있어 보안이 중요합니다. Check Point 게이트웨이는 발신·수신자가 제대로 된 위치에 있고 통화 권한이 있는지 확인하고, 패킷 내용을 검사해 구조적으로 유효하며 올바른 순서로 도착하는지(full stateful inspection) 확인합니다(VoIP 보안 개요).

네 가지 VoIP 프로토콜

게이트웨이가 보호하는 VoIP 프로토콜은 넷입니다. **SIP(Session Initiation Protocol)** — HTTP 유사 요청/응답 모델의 peer-to-peer 프로토콜, UDP/TCP 5060(평문)·5061(TLS) 사용 으로 가장 널리 쓰입니다(SIP). **H.323** — ITU 표준 기반의 전통적 VoIP 프로토콜 (H.323), **MGCP(Media Gateway Control Protocol)** — 게이트웨이를 중앙에서 제어하는 프로토콜 (MGCP), **SCCP(Skinny Client Control Protocol)** — Cisco의 경량 프로토콜 (SCCP)입니다.

보안·구성 용어

VoIP 트래픽은 통화 제어로 협상된 포트로 미디어가 동적으로 흐르 므로, 게이트웨이가 시그널링을 추적해 그에 맞는 미디어 연결을 동적으로 허용 해야 합니다. 이 동작은 Security Gateway의 stateful inspection 위에 얹히며, 구성은 SmartConsole에서 합니다(VoIP 구성). 진단에는 **Check Point Kernel Table** 이 쓰입니다(참조).

02 VoIP 보안 개요

VoIP 보안 개요

VoIP(Voice over IP) 통화는 복잡한 프로토콜이 여러 포트를 통해 오가 므로, 그 통로가 보안의 약점이 되기 쉽습니다. Check Point 게이트웨이는 SIP·H.323·MGCP·SCCP 환경의 VoIP 트래픽을 안전하게 통과 시킵니다.

게이트웨이가 하는 일

게이트웨이는 VoIP 통화에 대해 여러 검사를 합니다. 발신·수신자 주소가 있어야 할 곳에 있는지, 그들이 통화를 걸고 받을 권한이 있는지 확인하고, 패킷 내용을 들여다봐 허용된 정보만 담겼는지 봅니다. 무엇보다 SIP·H.323·MGCP·SCCP 명령에 대한 full stateful inspection 으로, 모든 VoIP 패킷이 구조적으로 유효하고 올바른 순서로 도착하는지 확인합니다.

왜 까다로운가

VoIP가 일반 트래픽보다 보호하기 까다로운 이유가 있습니다. 기술과 표준에서 보듯 통화 제어(시그널링)로 미디어가 흐를 포트를 동적으로 협상 하기 때문입니다. 즉 미디어(음성)가 미리 정해진 고정 포트가 아니라, 통화마다 협상된 포트로 흐릅니다. 그래서 게이트웨이는 시그널링을 추적해, 그 통화가 쓰기로 한 미디어 연결만 동적으로 허용 해야 합니다 — 고정 규칙만으로는 안 되고 stateful inspection이 필요한 이유입니다.

이 가이드는 VoIP가 게이트웨이를 지날 때 어떻게 구성하는지 를 프로토콜별로 설명합니다. 큰 줄기는 배포 형태(Deployments) → 기술·표준(Technology) → 프로토콜별 보안(SIP·MGCP·H.323·SCCP) → 구성(Configuring) 입니다.

03 VoIP 보안 배포

VoIP 보안 배포

게이트웨이를 VoIP 환경의 어디에 두느냐 에 따라 보호 방식이 달라집니다. 이 장은 대표적인 VoIP 보안 배포 형태를 정리합니다.

배포의 핵심 고려

VoIP 배포에서 중요한 것은 VoIP 구성요소(전화기·IP PBX·게이트키퍼·미디어 게이트웨이 등)가 게이트웨이를 기준으로 어디에 위치 하느냐입니다. 통화 제어 서버와 단말이 같은 쪽(내부)에 있는지, 게이트웨이를 사이에 두고 나뉘어 있는지 에 따라, 게이트웨이가 시그널링·미디어를 어떻게 추적·허용할지가 정해집니다.

전형적인 배포는 내부 VoIP 단말과 외부(인터넷·다른 사이트)의 단말·서버 사이에 게이트웨이를 두어, 그 사이 VoIP 트래픽을 검사 하는 형태입니다. NAT가 끼면 VoIP 주소가 패킷 본문(payload)에도 들어 있어, 게이트웨이가 시그널링 본문 안의 주소까지 함께 변환 해야 통화가 성립합니다.

정리하면, VoIP 배포 계획의 핵심은 VoIP 구성요소의 위치와 게이트웨이의 검사 지점을 맞추는 것이며, 그 위에서 프로토콜별 보안을 구성합니다. 구체적 배포 다이어그램·시나리오는 원문 해당 절을 참고하세요.

04 VoIP 기술과 표준

VoIP 기술과 표준

VoIP 프로토콜들을 이해하려면 통화가 어떤 신호로 이뤄지는지 부터 알아야 합니다. 이 장은 미디어·제어 신호와 VoIP가 다루는 기능을 정리합니다.

미디어 신호와 제어 신호

일반 디지털 전화든 VoIP든, 통화는 두 종류의 신호 로 이뤄집니다. **Media(미디어) 스트림**은 실제 음성 대화 이고, **Control(제어) 신호**는 다이얼 톤·벨소리처럼 통화 제어 과정을 나타냅니다.

VoIP 프로토콜들은 기술은 매우 다르지만 같은 목표 를 가집니다 — 통화를 제어하고 미디어를 흘리는 것입니다. 이들이 다루는 기능은 두 갈래입니다.

Call Control(시그널링) — 통화를 만들고·수정하고·끊는 제어 를 담당합니다.
Media·Gateway Control — 실제 음성 미디어의 흐름과 미디어 게이트웨이 제어 를 담당합니다. 프로토콜에 따라 이 두 기능을 한 프로토콜이 다 하거나, 시그널링과 미디어 제어를 나눠 맡깁니다.

표준

VoIP는 표준 기반입니다 — SIP는 여러 RFC와 표준 을 따르고, H.323은 ITU 표준, MGCP·SCCP도 각자의 규격을 따릅니다. Check Point 게이트웨이는 이 표준들을 stateful inspection으로 검증 해, 표준에 어긋나는 패킷을 걸러냅니다.

핵심은 시그널링이 미디어가 흐를 포트를 동적으로 협상 한다는 점입니다(VoIP 보안 개요) — 그래서 게이트웨이는 시그널링을 이해해 그에 맞는 미디어 연결을 동적으로 허용합니다. 이어지는 장들이 각 프로토콜의 보안을 다룹니다.

05 SIP(Session Initiation Protocol)

SIP(Session Initiation Protocol)

SIP(Session Initiation Protocol) 는 오늘날 가장 널리 쓰이는 VoIP 시그널링 프로토콜 입니다. 이 장은 SIP의 동작과 게이트웨이에서의 보안 구성을 정리합니다.

SIP의 동작

SIP는 UDP·TCP로 전송되는 Application Layer 제어 프로토콜 로, 하나 이상의 참가자와 세션을 만들고·수정하고·끝내 는 peer-to-peer 프로토콜입니다. HTTP의 요청/응답 트랜잭션 모델과 비슷 한 설계를 씁니다.

포트는 정해져 있습니다 — SIP 클라이언트는 보통 포트 5060(비암호화 시그널링)·5061(TLS 암호화) 로 SIP 서버·엔드포인트에 연결합니다. 시그널링은 이 포트로 오가지만, 실제 음성 미디어(RTP)는 시그널링으로 협상된 동적 포트 로 흐릅니다(기술과 표준).

게이트웨이에서의 SIP 보안

게이트웨이는 SIP 시그널링을 stateful inspection으로 추적 해, 그 통화가 협상한 미디어 연결만 동적으로 허용 합니다(VoIP 보안 개요). 즉 5060/5061만 열어 두는 게 아니라, SIP 메시지를 이해해 그에 맞는 미디어 포트를 그 통화 동안만 엽니다.

구성은 SmartConsole에서 합니다 — 기본 SIP 구성과 SIP 전용 서비스(SIP-Specific services) 를 정의해, VoIP 규칙에서 씁니다. NAT 환경에서는 SIP 메시지 본문 안의 주소까지 변환 해야 통화가 성립합니다.

정리하면, SIP는 HTTP 유사 요청/응답으로 세션을 제어하는 peer-to-peer 프로토콜 이고, 게이트웨이는 시그널링(5060/5061)을 추적해 협상된 미디어를 동적으로 허용 함으로써 SIP 통화를 안전하게 통과시킵니다. 세부 구성·서비스는 원문 해당 절을 참고하세요.

06 MGCP 기반 VoIP

MGCP 기반 VoIP

MGCP(Media Gateway Control Protocol) 는 중앙의 Call Agent가 미디어 게이트웨이를 제어 하는 VoIP 프로토콜입니다. 이 장은 MGCP의 특징과 게이트웨이 보안을 정리합니다.

MGCP의 동작

MGCP는 master/slave 구조 입니다 — 중앙의 **Call Agent**(Media Gateway Controller)가 지능을 갖고, 단말 쪽 **Media Gateway** 는 그 명령을 따르는 형태입니다. SIP·H.323이 단말에 지능이 있는 peer-to-peer라면, MGCP는 통화 제어 지능을 중앙에 모은 점이 다릅니다.

이 구조에서 Call Agent가 미디어 게이트웨이에 "이 포트로 이 통화의 미디어를 보내라"고 명령 하고, 게이트웨이는 그에 따라 음성을 흘립니다. 시그널링과 미디어가 분리되어 있어, 게이트웨이는 MGCP 제어 메시지를 추적해 그에 맞는 미디어 연결을 허용 해야 합니다.

게이트웨이에서의 MGCP 보안

Check Point 게이트웨이는 MGCP 명령에 full stateful inspection 을 적용해(VoIP 보안 개요), 명령이 구조적으로 유효하고 올바른 순서 인지 확인하고, Call Agent가 협상한 미디어 포트만 동적으로 엽니다. 발신·수신자의 위치와 권한도 함께 확인합니다.

정리하면, MGCP는 중앙 Call Agent가 미디어 게이트웨이를 제어하는 master/slave 프로토콜 이고, 게이트웨이는 MGCP 제어 메시지를 검사해 협상된 미디어를 안전하게 허용 합니다. 세부 구성은 원문 해당 절을 참고하세요.

07 H.323 기반 VoIP

H.323 기반 VoIP

H.323 은 ITU가 정한 전통적인 VoIP·멀티미디어 통신 프로토콜 묶음 입니다. 이 장은 H.323의 특징과 게이트웨이 보안을 정리합니다.

H.323의 동작

H.323은 하나의 프로토콜이 아니라 여러 하위 프로토콜의 묶음(suite) 입니다 — 통화 시그널링(H.225), 미디어 제어(H.245), 게이트키퍼 등록·허가(RAS) 등이 함께 동작합니다. 그래서 SIP보다 구조가 복잡하고, 여러 채널·포트를 동적으로 씁니다.

핵심 요소가 **Gatekeeper** 입니다 — 주소 변환, 통화 허가(admission), 대역폭 관리 를 담당하는 중앙 요소입니다. 단말은 게이트키퍼에 등록(RAS)하고, 통화 시그널링(H.225)으로 통화를 설정한 뒤, H.245로 미디어 채널을 협상해 음성을 흘립니다.

게이트웨이에서의 H.323 보안

H.323은 여러 프로토콜·채널이 얽혀 동적 포트를 많이 쓰므로, 게이트웨이의 추적이 특히 중요합니다. Check Point 게이트웨이는 H.225·H.245·RAS 메시지를 full stateful inspection 으로 따라가(VoIP 보안 개요), 협상된 시그널링·미디어 채널만 동적으로 허용 하고 각 메시지가 유효한지 확인합니다.

정리하면, H.323은 H.225·H.245·RAS·Gatekeeper로 이뤄진 ITU 표준 묶음 으로 구조가 복잡하고, 게이트웨이는 이 여러 프로토콜을 함께 추적해 동적 채널을 안전하게 허용 합니다. 세부 구성은 원문 해당 절을 참고하세요.

08 SCCP 기반 VoIP

SCCP 기반 VoIP

SCCP(Skinny Client Control Protocol) 는 Cisco가 만든 경량 VoIP 프로토콜 입니다(흔히 "Skinny"라 부름). 이 장은 SCCP의 특징과 게이트웨이 보안을 정리합니다.

SCCP의 동작

SCCP는 단말(IP 전화기)을 가볍게(skinny) 만들고, 통화 제어 지능을 중앙 서버에 모은 프로토콜입니다 — Cisco 환경에서 IP 전화기와 Call Manager(CUCM) 사이 의 통신에 쓰입니다. MGCP처럼 단말은 단순하고 중앙이 제어 하는 방식으로, 단말의 부담을 줄입니다.

전화기는 Call Manager에 등록하고, 통화 제어를 SCCP로 주고받으며, 실제 음성 미디어(RTP)는 협상된 포트로 흐릅니다.

게이트웨이에서의 SCCP 보안

Check Point 게이트웨이는 SCCP 명령에 full stateful inspection 을 적용해(VoIP 보안 개요), SCCP 제어 메시지를 추적해 협상된 미디어 연결만 동적으로 허용 하고, 발신·수신자의 위치·권한과 메시지 유효성을 확인합니다.

정리하면, SCCP는 Cisco의 경량 프로토콜로 단말은 단순하고 중앙(Call Manager)이 제어 하며, 게이트웨이는 SCCP 제어를 검사해 협상된 미디어를 안전하게 허용 합니다. 이렇게 SIP·H.323·MGCP·SCCP 네 프로토콜 모두를 같은 원리(시그널링 추적 → 동적 미디어 허용)로 보호합니다. 세부 구성은 원문 해당 절을 참고하세요.

09 VoIP 구성

VoIP 구성

앞에서 본 프로토콜별 보안을 실제 게이트웨이에 적용 하는 방법을 정리합니다.

Check Point 게이트웨이에서 VoIP 구성

VoIP 구성은 SmartConsole에서 합니다. 큰 줄기는 VoIP 구성요소(전화기·IP PBX·게이트키퍼·Call Agent 등)를 네트워크 객체로 정의 → 쓰는 프로토콜(SIP·H.323·MGCP·SCCP)에 맞는 서비스 객체 사용 → Access Control 규칙으로 VoIP 트래픽 허용 → 정책 설치 입니다.

핵심은 고정 미디어 포트를 일일이 열지 않는다 는 점입니다(VoIP 보안 개요). 시그널링 서비스(예: SIP)만 규칙에 허용하면, 게이트웨이가 시그널링을 추적해 그 통화의 미디어 연결을 동적으로 허용 합니다. 그래서 규칙은 단순하게 두고, stateful inspection이 동적 포트를 처리합니다.

NAT가 끼면 추가 고려가 있습니다 — VoIP 시그널링 본문(payload)에 IP·포트가 들어 있어, 게이트웨이가 헤더뿐 아니라 본문 안의 주소까지 변환 해야 통화가 성립합니다. Check Point는 이를 자동으로 처리합니다.

정리하면, VoIP 구성은 구성요소를 객체로 만들고, 시그널링을 허용하는 규칙만 두면 미디어는 게이트웨이가 동적으로 허용 하는 식입니다. 프로토콜별 세부 설정·옵션은 SIP·H.323·MGCP·SCCP 장과 원문 해당 절을 참고하세요.

10 참조 — 커널 테이블·명령줄

참조 — 커널 테이블·명령줄

VoIP를 진단하고 명령줄로 다루는 참조 자료를 정리합니다.

Check Point Kernel Table

게이트웨이가 VoIP 통화를 추적하는 상태는 **Kernel Table(커널 테이블)** 에 담깁니다. VoIP 보안 개요에서 봤듯, 게이트웨이는 시그널링을 추적해 협상된 미디어 연결을 동적으로 허용하는데, 그 통화·연결 상태가 커널 테이블에 기록됩니다.

VoIP가 의도대로 통과하지 않으면, 커널 테이블을 들여다봐 게이트웨이가 통화·미디어 연결을 제대로 추적하는지 확인합니다(`fw tab` 명령으로 테이블 조회). 이것이 VoIP 문제 해결의 출발점입니다.

명령줄·커널 참조

VoIP 관련 명령은 **R82 CLI Reference Guide** 와 원문 Command Line Reference 절에 정리되어 있습니다. 더 깊은 진단을 위한 **Working with Kernel Parameters·Kernel Debug** 는 Security Gateway 가이드의 명령줄·커널 참조·Performance Tuning 가이드와 같은 공통 주제이니 그쪽을 참고하세요.

정리하면, VoIP 진단은 커널 테이블(`fw tab`)로 통화·미디어 추적 상태를 확인 하는 것에서 시작하며, 깊은 분석은 커널 디버그로 합니다. 전체 명령은 R82 CLI Reference Guide가 담당합니다.