IPS Plugin

IPS Plugin 은 자동화된 IP 업데이트 및 차단 시스템을 통해 반복 공격으로부터 고객의 네트워크를 효과적으로 보호합니다. 리소스 낭비를 최소화하고, 운영 효율성과 보안 수준을 동시에 향상시키는 혁신적인 솔루션 입니다.

침입 방지 시스템(IPS : Intrusion Prevention System)

침입 방지 시스템(IPS)은 조직이 악성 트래픽을 식별하고 그러한 트래픽이 네트워크에 유입되는 것을 사전에 차단할 수 있도록 도와줍니다.

IPS 기술을 사용하는 제품은 인라인으로 배포하여 들어오는 트래픽을 모니터링하고 해당 트래픽에 취약성과 악용이 있는지 검사한 다음, 탐지가 되면 액세스 차단합니다.

문제 정의

지속적인 사이버 위협: 동일한 IP에서 반복적으로 발생하는 공격으로 인해 네트워크 리소스 낭비 증가.

기존 대응 방식의 한계: 실시간 탐지 후 차단 과정에서 과도한 시스템 부하 및 관리 비용 발생.

Time	Level	Threat Level	Sub Type	Source	Destination	Action	Service	Message
07-25 18:09:32(+0900)	[redacted]	critical	ips	112.184.186.219	172.16.1.2	dropped	HTTP	applications3: Zyxel.zhttpd.Webserver.Command.Injection,
07-25 16:11:55(+0900)	[redacted]	critical	ips	118.49.115.236	10.100.0.2	dropped	HTTP	applications3: Zyxel.zhttpd.Webserver.Command.Injection,
07-25 00:12:23(+0900)	[redacted]	critical	ips	125.139.48.244	10.100.0.2	dropped	HTTP	applications3: Zyxel.zhttpd.Webserver.Command.Injection,
07-24 19:08:42(+0900)	[redacted]	critical	ips	121.152.45.18	10.100.0.2	dropped	HTTP	applications3: Zyxel.zhttpd.Webserver.Command.Injection,
07-24 16:35:11(+0900)	[redacted]	critical	ips	118.41.39.138	172.16.1.2	dropped	HTTP	applications3: Zyxel.zhttpd.Webserver.Command.Injection,
07-24 16:26:21(+0900)	[redacted]	critical	ips	121.146.38.221	10.100.0.2	dropped	HTTP	applications3: Zyxel.zhttpd.Webserver.Command.Injection,
07-24 14:59:35(+0900)	[redacted]	critical	ips	220.124.239.53	172.16.1.2	dropped	HTTP	applications3: Zyxel.zhttpd.Webserver.Command.Injection,
07-24 11:01:35(+0900)	[redacted]	critical	ips	59.15.62.17	10.100.0.2	dropped	HTTP	applications3: Zyxel.zhttpd.Webserver.Command.Injection,
07-22 08:53:22(+0900)	[redacted]	critical	ips	14.47.213.111	10.100.0.2	dropped	HTTP	applications3: Zyxel.zhttpd.Webserver.Command.Injection,
07-21 23:31:22(+0900)	[redacted]	critical	ips	125.142.6.137	10.100.0.2	dropped	HTTP	applications3: Zyxel.zhttpd.Webserver.Command.Injection,

[공격탐지 모니터링 결과]

IPS Plugin 의 핵심 기능

1) 지능형 IP 분석 및 차단

- Fortinet 장비에서 차단된 IP 정보를 실시간으로 수집 및 분석.
- 악성 트래픽을 유발하는 IP를 Fortinet 블록 리스트에 자동 등록하여 반복 공격을 원천 차단.

2) 시스템 리소스 절감

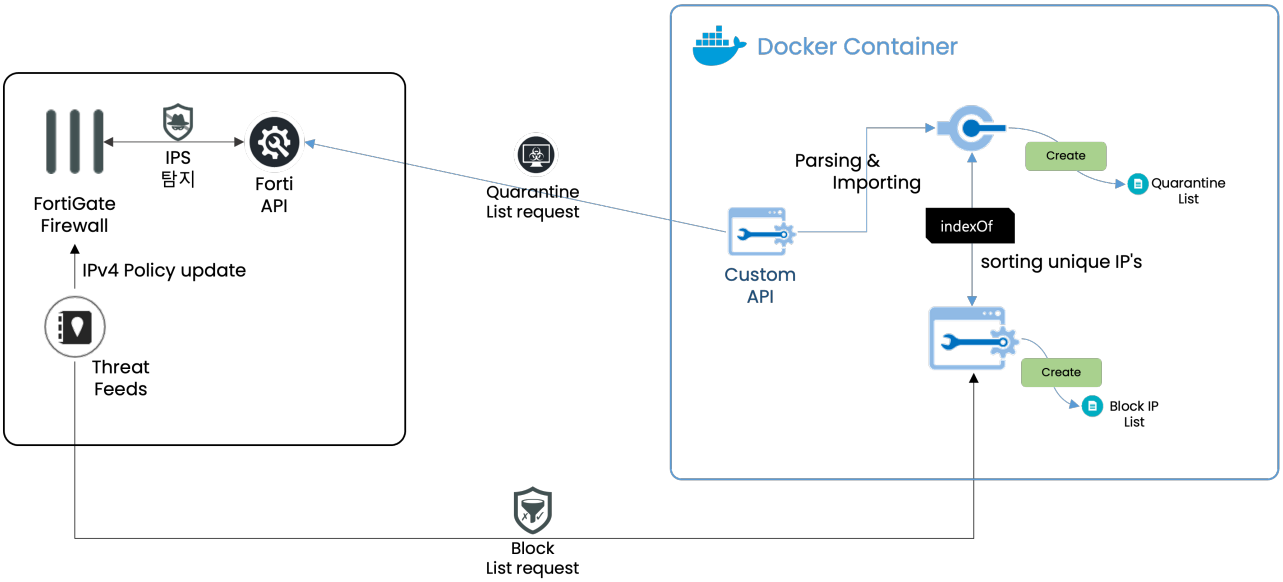
- 지속적인 공격에서 발생하는 시스템 과부하를 줄이고, 네트워크의 성능과 안정성을 유지.
- 관리자가 개입하지 않아도, 자동화된 방식으로 네트워크를 보호.

3) 최신 위협 대응

- 블록 리스트를 주기적으로 업데이트하여 최신 보안 위협에 선제 대응.
- FortiGuard와 연동해 위협 인텔리전스를 실시간으로 반영.

4) 효율적인 네트워크 관리

- 자동화된 운영으로 관리자의 부담을 줄이고 더 중요한 작업에 집중 가능.
- 보안 관리 프로세스가 간소화되어, 보안 인프라 운영이 더욱 효율적.



[IPS Plugin diagrams]

Fortinet IPS 도입 효과

1) 리소스 절감:

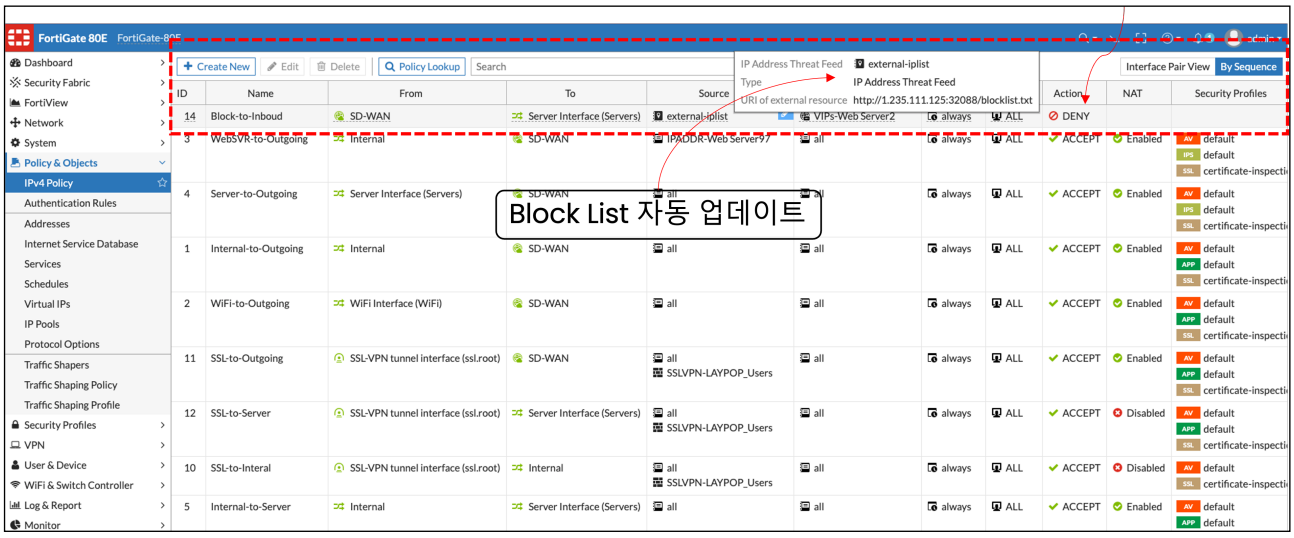
- 동일한 공격 시도를 초기 단계에서 차단해 네트워크 및 장비의 부하 감소.
- 방화벽 및 기타 보안 장비의 처리 용량 최적화.

2) 보안 강화:

- 반복적인 악성 IP로 인한 위협 차단으로 네트워크 무결성 유지.
- 악성 활동의 확산 방지 및 잠재적 피해 최소화.

3) 운영 효율성 향상:

- 수동 관리 작업 감소: 자동 업데이트 및 차단 프로세스를 통한 운영 간소화.



- 보고서를 통해 위협 동향 및 대응 상태 투명하게 확인 가능.

[FortiGate Threat Feeds]