WHITE PAPER

Proteggere l'ecosistema IoT con Fortinet

L'impatto potenziale di un attacco informatico riuscito su un ecosistema IoT può provocare la compromissione di sistemi e settori critici e persino un pericolo fisico per le persone e l'ambiente. È quindi importante che i fornitori di soluzioni per l'IoT dimostrino il loro impegno a fornire un servizio che sia intrinsecamente sicuro già a livello di progettazione.

I fornitori di servizi gestiti (MSP), i fornitori di servizi di sicurezza gestiti (MSSP) e gli operatori di reti mobili (MNO) devono garantire la sicurezza come parte delle loro soluzioni e servizi IoT per raggiungere tre obiettivi principali:

1. Proteggere l'intero ecosistema IoT in modo da garantire la continuità del servizio
2. Fornire SLA per la sicurezza dell'IoT in modo da incoraggiare l'adozione e l'accettazione dei servizi IoT
3. Fornire servizi di sicurezza IoT che generino ricavi

Soluzione di sicurezza Fortinet per l'IoT

La soluzione Fortinet per l'IoT consiste in una serie di componenti di sicurezza basati sulle best practice che insieme garantiscono una protezione completa a un ecosistema IoT. Poiché il termine IoT è di per sé ampio, qualsiasi soluzione deve essere costituita da un ampio set di funzionalità integrate e automatizzate, che possono essere applicate in base alle esigenze di ogni singolo caso d'uso.

Le funzionalità di sicurezza Fortinet per l'IoT sono fornite attraverso la più completa gamma di prodotti per la sicurezza di rete del settore, interconnessi e integrati all'interno del suo Security Fabric per fornire servizi di sicurezza e una potente piattaforma per la sicurezza dell'ecosistema IoT end-to-end.

Le funzionalità di sicurezza di Fortinet per l'IoT sono passano per il firewall di nuova generazione FortiGate (NGFW) e il firewall per applicazioni web FortiWeb, entrambi offerti in versione fisica e virtuale.

FortiGate: segmentazione e firewalling stateful

In molti casi, i modelli di traffico di un dispositivo IoT sono molto predicibili e un firewall stateful FortiGate può bloccare qualsiasi traffico indirizzato a destinazioni non autorizzate, oltre a segnalare che il dispositivo si comporta in modo anomalo. In un tipico ambiente IT, il traffico verso destinazioni non autorizzate può essere comune per molte ragioni, e generalmente tali comunicazioni verrebbero semplicemente interrotte. Nell'Internet Of Things e in altre reti macchina-macchina, invece, tali comunicazioni sono solitamente un segno di errata configurazione o compromissione. Per questo motivo, occorre configurare specifiche regole negative con un'azione appropriata per garantire che venga generato un allarme o venga attivato un rimedio automatico.

FortiGate: prevenzione delle intrusioni

L'Intrusion Prevention Service del FortiGate è progettato per rilevare e bloccare un'ampia gamma di attacchi IoT, tra cui:

- **Exploit:** questa categoria include qualsiasi attacco a una vulnerabilità ed è generalmente utilizzato per causare un Denial-of-Service (DoS) (provocando un crash o un lavoro extra all'interno del software) oppure l'esecuzione di codice locale che spesso si traduce in un attacco di secondo livello come il trasferimento di un eseguibile dannoso.
- **Attacchi di scansione:** in questa categoria rientrano la ricerca di porte TCP (Transmission Control Protocol) o UDP (User Datagram Protocol) aperte oppure la ricerca di software o versioni di protocollo note. Di solito, l'obiettivo degli attacchi di ricognizione è l'identificazione di obiettivi vulnerabili od obiettivi di alto valore.
- **Attacchi di fuzzing:** questo è un altro metodo per trovare le vulnerabilità. Di norma, viene sferrato localmente in un ambiente controllato, ma può essere utilizzato come blunt-instrument attack su una rete live. Ne sono un esempio le anomalie di protocollo intenzionali o l'utilizzo di campi estremamente lunghi o dati non validi o insoliti. Tutte queste tecniche sono volte a innescare errori di programmazione con l'obiettivo di individuare vulnerabilità o semplicemente provocare un'interruzione.

Questi tipi di attacco e molti altri sono coperti dalla funzione di intrusion prevention (IPS) del FortiGate, che contiene più di 30.000 regole, compreso un pacchetto industriale opzionale. I pacchetti di regole vengono aggiornati automaticamente ogni giorno per garantire una protezione costantemente aggiornata.

L'IPS Fortinet ha anche la capacità di definire regole basate sul rate, e poiché molti dispositivi IoT hanno un rate di pacchetti predicibile, la funzione può essere utilizzata per rilevare attività insolite, eventualmente causate da malfunzionamenti o compromissioni, e rimuovere tali dispositivi dalla rete.

Vi è una tendenza generale in tutti i settori del networking verso la crittografia dei dati, e questo vale anche per l'Internet degli oggetti, dove i dati sono spesso di natura privata. Nella maggior parte dei casi, si utilizza il protocollo TLS e l'IPS può eseguire un'ispezione TLS per consentire il rilevamento di attacchi su tali collegamenti sicuri.

FortiGate: controllo di protocolli e applicazioni

La funzione Application Control può essere usata per monitorare o limitare i protocolli utilizzabili dal dispositivo IoT. Qualsiasi protocollo non autorizzato può generare un allarme ed essere eventualmente bloccato. Le definizioni delle applicazioni includono più di 4.000 regole in 24 categorie. Sono coperti tutti i protocolli IoT più comuni come MQTT, AMQP, HTTP e CoAP, e come nel caso dell'IPS, si può usare l'ispezione TLS con una configurazione appropriata. È anche disponibile una vasta gamma di protocolli industriali per le soluzioni Industrial Internet-of-Things (IIoT).

Antivirus

Fortinet ha una soluzione antivirus ormai collaudata, supportata dalla ricerca FortiGuard Labs e dall'elaborazione basata sull'intelligenza artificiale (AI). Grazie all'abbinamento con la funzione di prevenzione delle intrusioni, la stragrande maggioranza dei file dannosi non potrà mai raggiungere l'obiettivo.

Oggi l'antivirus è importante soprattutto per l'infrastruttura IoT, come i server web o di piattaforme, ma secondo i ricercatori, il malware rivolto contro gli stessi dispositivi (come il malware IoT Mirai, forse l'esempio attuale più famoso) diventerà più prevalente negli anni a venire.

FortiGuard Labs ha maturato quasi 20 anni di esperienza nella difesa contro il malware di ogni tipo e, nonostante il fatto che il malware mirato ai dispositivi sia oggi raro, sono già in corso gli studi necessari per garantire la massima protezione.

Anti-botnet

Qualsiasi attività della rete bot, sia essa rilevata per indirizzo di destinazione, dominio o protocollo, può generare un avviso ed essere bloccata. Inoltre, le connessioni ad altre destinazioni note cattive, come rilevate dagli Indicatori FortiGuard del Servizio Compromesso, possono generare un avviso di compromesso. FortiGuard Labs mantiene un elenco aggiornato di combinazioni note di indirizzi di destinazione e porte botnet che vengono controllate rispetto a tutte le sessioni in uscita. Le botnet che utilizzano domini a flusso rapido (in cui un dominio cambia continuamente la mappatura degli indirizzi IP) possono essere controllate rispetto al dominio stesso intercettando e controllando la richiesta del Domain Name System (DNS). Infine, anche se l'indirizzo di destinazione e il dominio sono sconosciuti, molte botnet possono essere riconosciute dal loro protocollo di comando e controllo. Utilizzando questi tre metodi in parallelo, Fortinet garantisce le migliori possibilità di rilevare dispositivi infetti da botnet.

Protezione API con FortiWeb

Le API sono utilizzate in più ambiti nelle reti IoT. In generale, le interazioni tra i dispositivi e le piattaforme IoT avvengono tramite API, di solito con protocolli come MQTT, HTTP e CoAP, e utilizzando JSON o XML come codifica dei dati (per ambienti ad alta compressione e larghezza di banda bassa si utilizzano codifiche binarie come CBOR). Le API servono inoltre per la comunicazione tra le applicazioni e la piattaforma IoT, di norma utilizzando l'HTTP.

Fortinet ha una funzione di protezione delle API molto forte in FortiWeb, che permette di definire una vasta gamma di vincoli, da semplici regole come la lunghezza massima dell'intestazione e del campo, fino alla validazione e all'applicazione dello schema, utilizzando sostanzialmente l'HTTP con JSON o XML.

Unitamente a FortiWeb, è possibile attenuare sia gli attacchi generici sia quelli mirati contro le API REST e i web front-end.

Automazione

Fortinet ha un framework di automazione completo che permette di collegare un'ampia gamma di trigger ad azioni come allarme, rimozione di dispositivi rogue dalla rete o esecuzione di chiamate API verso altri dispositivi.

Ad esempio, uno qualsiasi dei rilevamenti di cui sopra può causare la messa in quarantena di un dispositivo e il blocco di ulteriori comunicazioni fino a quando la causa non viene appurata e non vengono adottate misure correttive.

Il Fortinet Security Fabric

Sono tante e diverse le sfide poste alla sicurezza dell'IoT, e un insieme eterogeneo di prodotti puntuali indipendenti inevitabilmente le moltiplica in termini di complessità operativa.

Il Security Fabric di Fortinet è stato progettato per superare queste difficoltà integrando i componenti di sicurezza con l'obiettivo di garantire che i dispositivi funzionino in modo coerente, condividendo la threat intelligence e garantendo visibilità e reporting unificati, elaborazione e analisi aggregata dei log e gestione da un'unica interfaccia. Le soluzioni Fortinet per l'IoT fanno parte delle funzionalità complessive che il Security Fabric fornisce a imprese, MSP, MSSP e MNO.

In futuro: integrazione con i partner tecnologici

Aptilo e Fortinet: un servizio di controllo della connettività per l'IoT

Il Security Fabric di Fortinet si estende anche a una serie accuratamente selezionata di prodotti di terzi che fanno parte del programma Fortinet Fabric-Ready. Ognuna di queste partnership è stata sviluppata per garantire un'integrazione di alta qualità con il fabric per prodotti che creano un valore reale per la soluzione nel suo complesso.

Fortinet ha collaborato con diversi partner tecnologici per integrare le loro soluzioni per l'IoT, completando e migliorando la capacità dei fornitori di servizi di comunicazione (CSP) di mettere a disposizione dei loro clienti aziendali un'ampia gamma di servizi innovativi per l'IoT. Questo ecosistema di soluzioni pre-integrate garantisce un onboarding rapido ed efficace di una gamma sempre più ampia di servizi IoT integrati.

Il Connectivity Control Service (CCS) per l'IoT di Aptilo è un esempio di integrazione del Security Fabric per l'IoT e del valore aggiunto che è in grado di fornire ai MNO.

L'IoT CCS consente ai MNO di superare alcuni limiti dei core di pacchetti mobili (anche potenziati) quando si cerca di creare servizi IoT flessibili su larga scala, tra cui:

- Complessità nell'offrire APN privati (connessione di rete privata virtuale [VPN]) alle aziende su larga scala
- Incapacità di offrire servizi di sicurezza per l'IoT al di là degli APN
- Impossibilità di effettuare l'onboarding automatico di nuovi clienti
- Difficoltà per i clienti nel gestire le proprie policy di sicurezza e connettività
- Impossibilità nel fissare policy univoche per ciascun cliente, quindi tantomeno per ciascun dispositivo
- Difficile nel configurare APN per più stakeholder dallo stesso dispositivo
- Difficoltà nell'ottenere una connettività IoT globale senza roaming e con breakout del traffico basato su policy

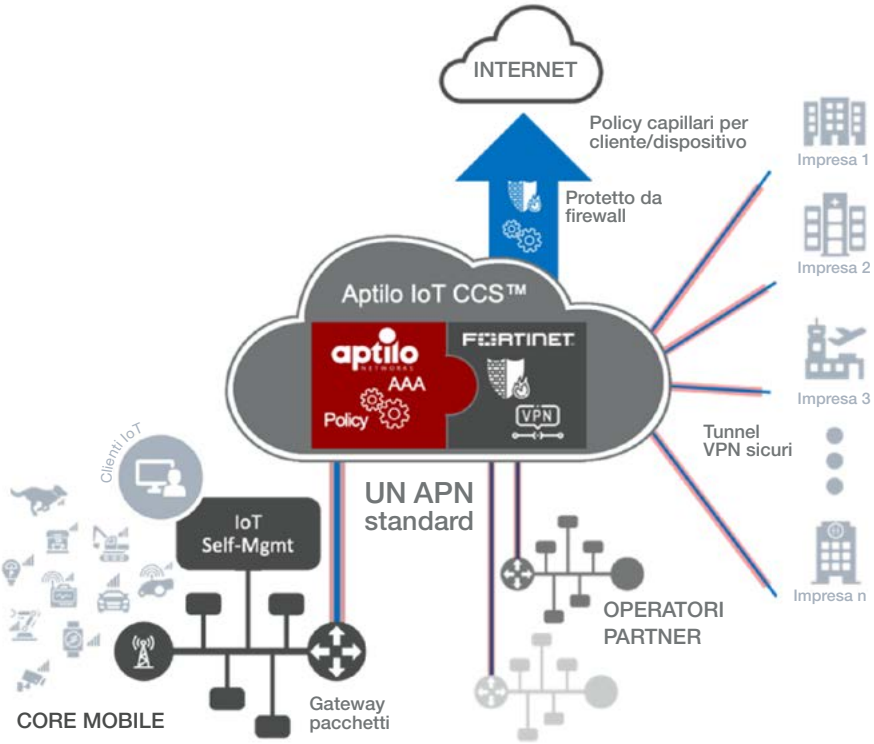
Con la soluzione congiunta Fortinet e Aptilo, gli operatori di reti mobili possono lasciare intatto il loro core mobile e creare servizi di connettività IoT prima considerati irrealizzabili. L'IoT CCS fornito come servizio su Amazon AWS (OPEX) offre un controllo flessibile della connettività IoT e un livello di sicurezza superiore a qualsiasi core mobile attuale e futuro. Gli operatori mobili possono fornire servizi innovativi di connettività IoT in pochi giorni anziché in mesi, a un costo molto più contenuto rispetto alle alternative disponibili.

FortiGate, la famiglia di firewall per reti Fortinet, gestisce la sicurezza e il traffico/data plane dell'IoT CCS. Attraverso il FortiGate, l'IoT CCS ottiene l'applicazione delle policy lungo il perimetro, il routing, la gestione delle VPN, il traffic filtering dei dispositivi, la protezione dagli attacchi DDoS (Distributed Denial-of-Service), la limitazione del numero di connessioni TCP e molto altro. Anche il rilevamento delle anomalie fa parte del livello di sicurezza dell'IoT CCS.

L'APN virtuale multi-tenancy dell'IoT CCS elimina la complessità derivante dalla configurazione di singoli APN privati per ogni cliente aziendale attribuendo **un solo** APN standard all'IoT CCS che è al servizio di **tutte le** imprese collegate. Il provisioning delle VPN avviene automaticamente tramite un'API, rendendo l'onboarding di nuovi clienti un gioco da ragazzi.

Con lo stesso APN, gli operatori di reti mobili possono aggiungere al loro servizio IoT CCS operatori di reti mobili internazionali loro partner, e sfruttando la loro capacità di localizzare istantaneamente eSIM (eUICC) via etere, possono offrire una connettività veramente globale e sicura senza costi di roaming.

Attraverso l'APN virtuale multi-tenancy dell'IoT CCS, gli operatori possono offrire una connettività internazionale sicura con breakout opzionale per il traffico selezionato nel punto di presenza AWS più vicino, offrendo prestazioni ottimizzate attraverso l'uso delle funzionalità SD-WAN (Software-Defined Wired-Area Network) FortiGate, funzionalità uniche che è praticamente impossibile ottenere nel core 3GPP standard con l'home routing come opzione tipica.



In sintesi

L'IoT sta cambiando il mondo in cui viviamo offrendoci enormi opportunità, ma anche ponendoci notevoli sfide. I CSP hanno un ruolo essenziale da svolgere per rendere possibile e proteggere l'ecosistema IoT per i loro clienti.

Fortinet è in una posizione ideale per salvaguardare le diverse esigenze dei servizi e dell'ecosistema IoT, dalle imprese ai fornitori di servizi. Con prestazioni carrier-grade, multi-tenancy e modelli di consumo flessibili, Fortinet fornisce ai CSP una piattaforma di sicurezza per l'IoT che proteggere i servizi IoT e i ricavi, consentendo al tempo stesso ai clienti di realizzare la promessa dell'IoT.

febbraio 16, 2021 10:42 AM

785701-0-1-IT