SOLUTION BRIEF

Visibilità approfondita per applicazioni, utenti e dispositivi con i Next-Generation Firewall FortiGate

Executive Summary

I firewall tradizionali sono in genere in grado di consentire o bloccare le connessioni solo in base alla porta e al protocollo. Tuttavia, l'accesso alla rete è ora dinamico e contestuale, operando secondo i principi dell'approccio zero-trust. Inoltre, l'azienda moderna è ibrida, con data center on-premise, cloud pubblici, filiali e campus aziendali, nonché sedi remote. I team IT di oggi hanno bisogno di una visibilità approfondita sulle applicazioni, gli utenti e i dispositivi per difendere le reti aziendali dalle minacce informatiche in tutto l'ambiente, ma questo in genere comporta tutta una serie di problematiche.

Ad aggravare il problema della visibilità c'è il fatto che quasi tutto il traffico Internet è ormai crittografato. Le aziende si ritrovano con ampi punti ciechi della rete, man mano che passano da costose architetture hub-and-spoke a modelli distribuiti con accesso diretto a Internet nelle varie sedi. Gli utenti malintenzionati possono sfruttare queste lacune della rete, occultando le minacce nel traffico crittografato.

Oltre il 95% del traffico internet è ora crittografato.[1]

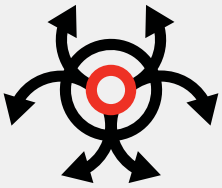
I Next-Generation Firewall (NGFW) FortiGate offrono visibilità sul traffico crittografato e sulle attività di utenti, applicazioni e dispositivi, necessaria per creare policy di rete e di sicurezza contestuali e in continua evoluzione, per garantire la trasformazione digitale. Gli NGFW FortiGate sono in grado di identificare e controllare tutti gli utenti, le applicazioni e i dispositivi presenti sulla rete, grazie a tecniche avanzate di raccolta e analisi dei dati. Come componente chiave di una soluzione HMF (Hybrid Mesh Firewall), gli NGFW FortiGate integrano queste funzionalità di visibilità e protezione in tutti i domini IT, coprendo l'intera infrastruttura di rete.

Application Control

Il servizio FortiGuard Application Control si collega agli NGFW FortiGate e identifica rapidamente le applicazioni note e sconosciute che transitano nella rete, consentendo di creare facilmente policy per autorizzare, negare e limitare l'accesso alle applicazioni, a determinate funzioni all'interno delle applicazioni e a categorie di applicazioni.

#	Rischio	Applicazioni	Categoria	Tecnologia	Utenti	Larghezza di banda	Sessione
1	5	Asprox.Botnet	Botnet	Client-Server	1	1.74 MB	587
2	5	Proxy.HTTP	Proxy	Network-Protocol	11	7.10 MB	457
3	5	Onavo.Protect	Proxy	Client-Server	1	1.78 KB	9
4	5	Hotspot.Shield	Proxy	Client-Server	2	203.99 KB	8
5	5	Skyfire	Proxy	Client-Server	3	27.20 KB	3
6	4	Rsh	Remote.Access	Client-Server	67	9.82 GB	302,237
7	4	BitTorrent	P2P	Peer-to-Peer	8	1.79 MB	5,096
8	4	Telnet	Remote.Access	Client-Server	9	37.81 MB	681
9	4	RDP	Remote.Access	Client-Server	14	9.89 MB	48
10	4	TeamViewer	Remote.Access	Client-Server	22	1.13 MB	38

I dispositivi NGFW FortiGate hanno la capacità di identificare le applicazioni non solo in base alla porta e al protocollo, ma anche utilizzando la signature delle applicazioni, i comportamenti euristici e altri indicatori di identificazione. Grazie all'analisi combinata delle signature delle applicazioni e del database dei servizi Internet (ISDB), FortiGate può impostare più di 4.200 regole di controllo delle applicazioni. Di seguito sono elencati alcuni dei metodi con cui FortiGate rileva le applicazioni oltre i livelli 3 e 4.



"...le aziende che hanno ispezionato il traffico in entrata hanno dichiarato che il 70% del malware deriva da una connessione crittografata".[2]

Signature delle applicazioni: Il traffico di rete autorizzato viene contrassegnato con una signature basata sulle caratteristiche della transazione e sulla presenza di una porta dell'applicazione predefinita o non standard. Questo traffico viene quindi sottoposto ad un'analisi approfondita alla ricerca di potenziali minacce.

Crittografia: se FortiGate rileva una crittografia come SSL (Secure Sockets Layer)/ TLS (Transport Layer Security), HTTPS (Hypertext Transfer Protocol Secure) o SSH (Secure SHell) e se è presente una regola di policy decrittografia, la sessione viene decrittografata e le signature delle applicazioni vengono applicate nuovamente al flusso decrittografato.

Decodificatori: nel caso in cui il protocollo dell'applicazione sia noto, vengono utilizzate signature aggiuntive basate sul contesto per rilevare altre applicazioni che potrebbero essere nascoste all'interno del protocollo stesso.I decodificatori convalidano la conformità del traffico alle specifiche del protocollo e forniscono supporto per la conversione degli indirizzi di rete (NAT, Network Address Translation) e per l'apertura di pinhole dinamici per applicazioni quali SIP (Session Initiation Protocol) e FTP (File Transfer Protocol).

Euristica: l'analisi euristica di FortiGate utilizza l'analisi comportamentale per determinare l'identità delle applicazioni elusive, tra cui le applicazioni che utilizzano la porta 80, la porta 443 o che effettuano il port hopping, ad esempio le applicazioni VoIP (Voice over Internet Protocol), di collaborazione e peer-to-peer (P2P) che non possono essere identificate tramite l'analisi avanzata delle signature e dei protocolli.

Se il FortiGate non è in grado di identificare un'applicazione in base alla sua signature, sfruttando l'euristica, si farà affidamento sulle caratteristiche comportamentali per classificare un'applicazione precedentemente sconosciuta all'interno di un gruppo di applicazioni esistenti. Inoltre, verranno applicati filtri dinamici o inoltro basato su policy per ottenere il risultato desiderato.

L'identificazione delle applicazioni può fornire un contesto significativo sulla rete. FortiGate è in grado di rivelare informazioni sulla funzione intrinseca, sulle porte delle applicazioni, sul protocollo, sulla tecnologia e sulle caratteristiche comportamentali dell'applicazione, consentendo ai team IT di definire policy di accesso sicure e visibili. Una volta che il team comprende come un'applicazione viene utilizzata sulla rete, è possibile applicare una serie di policy e risposte oltre l'autorizzazione e il blocco.

FortiGuard Application Control consente inoltre alle organizzazioni di creare policy e funzioni di controllo all'interno di ogni applicazione, ad esempio:

- Consentire l'accesso a Facebook ma bloccare i trasferimenti dei file di Facebook Messenger
- Permettere agli utenti di accedere a Gmail ma disabilitare Google Chat
- Bloccare il caricamento dei file su Dropbox, Box o Google Drive
- Filtrare la visualizzazione di categorie di video indesiderate su YouTube

FortiOS, il sistema operativo di FortiGate, fornisce un'ampia visibilità sull'utilizzo delle applicazioni in tempo reale, nonché sulle tendenze nel tempo tramite views, visualizzazioni e report. L'Application Control tiene fuori dalla rete le applicazioni dannose, rischiose ed indesiderate grazie a punti di controllo sul perimetro, nel data center e internamente tra i segmenti di rete.

Identificazione degli utenti

L'identificazione degli utenti al di là dei loro indirizzi IP è un'altra parte fondamentale della sicurezza aziendale. FortiOS può identificare gli utenti in base a una serie di origini e metodi, come Microsoft Active Directory (AD), server LDAP, syslog, mappatura delle porte e intestazioni XFF.

L'identificazione degli utenti di FortiGate offre una migliore visibilità delle attività di rete e il rilevamento di comportamenti dannosi o nocivi. L'identificazione degli utenti di FortiGate permette di riconoscere gli utenti su tutti i sistemi operativi, ovunque si trovino, offrendo una maggiore visibilità sull'utilizzo delle applicazioni in base agli utenti. Ciò consente ai team IT di avere una visione più completa e significativa delle attività di rete.

L'efficacia dell'identificazione degli utenti diventa chiara quando si rileva un'applicazione sconosciuta sulla rete. Utilizzando strumenti come FortiView o i log di Application Control, i team di sicurezza sono in grado di individuare:

- L'applicazione
- L'utente
- Il consumo della larghezza di banda e della sessione
- Origine e destinazione del traffico applicativo
- Eventuali minacce associate

Mappatura degli utenti

FortiGate è in grado di creare profili degli utenti della rete e di abbinare i nomi utente agli indirizzi IP dei pacchetti ricevuti. Le informazioni sugli utenti possono essere associate alle policy di sicurezza per un utilizzo più sicuro della rete, riservando l'accesso alle applicazioni solo a chi ne ha bisogno per motivi di lavoro. La mappatura degli utenti può consentire un set di regole o policy per le applicazioni meno rischiose, come Salesforce o PowerPoint, e allo stesso tempo impostare policy più rigorose per le applicazioni sensibili, come gli strumenti di pen-testing o i controller di desktop remoti.

Mappatura dei gruppi

La definizione di regole di policy basate sui gruppi di utenti può semplificare la gestione dell'IT, in quanto le policy e le regole sono già presenti e non devono essere riconfigurate quando si aggiungono nuovi utenti ai gruppi. FortiGate è in grado di applicare queste regole e gli aggiornamenti dei gruppi, supportando un'ampia gamma di server di directory, tra cui Microsoft AD, Novell eDirectory e Sun ONE Directory Server. Dopo aver abilitato l'identificazione degli utenti e aver sfruttato la mappatura dei gruppi, è possibile configurare le policy di sicurezza per utenti e gruppi specifici, tra cui categorie e sottocategorie di applicazioni, tecnologie sottostanti e caratteristiche delle applicazioni. È possibile definire regole di policy per abilitare in modo sicuro le applicazioni in base agli utenti e ai gruppi di utenti, sia in uscita che in entrata.

Esempi di policy basate su utenti e gruppi sono:

- Strumenti come SSH, Telnet e FTP su porte standard, riservati all'IT aziendale
- Policy come:
  - Consentire al reparto vendite di accedere a Salesforce e Microsoft 365
  - Consentire a tutti gli utenti di guardare YouTube, ma bloccare categorie di video specifiche

L'identificazione degli utenti permette di definire le policy che supportano e proteggono i dipendenti, gli ospiti e le altre parti interessate. FortiGate è in grado di fornire una visione approfondita degli utenti e di automatizzare i controlli delle policy.

Identificazione dei dispositivi

Mentre l'identificazione degli utenti fornisce policy basate sull'utente e l'identificazione delle applicazioni fornisce policy basate sull'applicazione, l'identificazione dei dispositivi fornisce regole di policy basate su un dispositivo, indipendentemente dalle modifiche al suo indirizzo IP o alla sua posizione. Fornendo la tracciabilità dei dispositivi e associando gli eventi di rete a dispositivi specifici, l'ID del dispositivo fornisce il contesto in cui gli eventi si riferiscono ai dispositivi. Scrive policy associate ai dispositivi invece che agli utenti, alle posizioni o agli indirizzi IP, che possono cambiare nel tempo. L'ID del dispositivo è importante per le policy di sicurezza, decrittografia, qualità del servizio (QoS) e autenticazione.

Con FortiGate, le policy avanzate dei dispositivi e l'assegnazione di priorità possono essere classificate come segue:

- Classe, ad esempio i dispositivi sicuri in rete
- Dispositivi critici, tra cui server e dispositivi medici
- Dispositivi ambientali, come lettori di badge, telecamere e allarmi antincendio
- Dispositivi Internet-of-Things (IoT), ad esempio smartwatch e altri dispositivi "smart" connessi

Decrittografia SSL/TLS 1.3

Poiché il malware si nasconde regolarmente nel traffico crittografato, è fondamentale che questo venga esaminato. Gli NGFW FortiGate offrono decrittografia SSL/TLS 1.3 senza rallentamenti di rete. Inoltre, i FortiGate possono decrittografare tipi specifici di traffico ed effettuare esclusioni in base a siti o categorie. Con le unità di elaborazione della sicurezza proprietarie ad alte prestazioni di Fortinet, non è necessario scegliere tra sicurezza e prestazioni.

Gestione centrale e unificata

La gestione centralizzata e unificata è la capacità più critica di un HMF. Se domini separati, come le sedi aziendali, i cloud pubblici, i cloud privati e i telelavoratori, richiedono una protezione tramite dashboard separati, la complessità dell'IT aumenta e la visibilità si riduce notevolmente.

La gestione centralizzata coordina e unifica i diversi domini di sicurezza in un'unica soluzione di sicurezza IT aziendale: una protezione semplice, unificata e automatizzata che si estende dalle sedi aziendali al cloud e ai lavoratori da remoto. Poiché le diverse aziende hanno requisiti diversi per la gestione dei firewall di rete dispersi, è necessario supportare tutti i fattori di forma della gestione centralizzata, comprese le appliance, le macchine virtuali, i SaaS e i servizi firewall gestiti.

La gestione centralizzata offre anche un enorme valore nel riunire i team dei NOC (Network Operations Center) e dei SOC (Security Operations Center) utilizzando un'unica interfaccia per gestire, monitorare e proteggere l'intera superficie di attacco.

FortiGuard AI-Powered Security Services

Con oltre 8 milioni di sensori distribuiti in tutto il mondo, gli NGFW FortiGate sono in grado di sfruttare la più recente threat intelligence globale tramite FortiGuard AI-Powered Security Services. Grazie agli aggiornamenti di sicurezza completi e in tempo reale, FortiGate è in grado di proteggere l'intera rete con difese di sicurezza a più livelli, come il filtraggio di URL e DNS, l'antimalware e il sandboxing in linea, nonché l'IPS accelerato da hardware per l'applicazione di patch virtuali ad alte prestazioni. Questi servizi di sicurezza informatica proteggono l'azienda sia dagli attacchi noti che da quelli precedentemente sconosciuti. I test indipendenti di CyberRatings.org[3] dimostrano che gli NGFW FortiGate hanno un'efficacia del 99,88% contro gli exploit e le elusioni dannose.

Conclusioni

L'identificazione di applicazioni, utenti e dispositivi sulla rete è una funzionalità importante per la gestione e la protezione delle reti aziendali. I FortiGate NGFW sono noti per la loro visibilità avanzata ed il controllo del traffico di rete, oltre che per le eccezionali prestazioni. FortiGate definisce ed automatizza le policy che assicurano l'uso appropriato, bloccano le minacce e riducono la superficie di attacco aziendale. La gestione centralizzata e unificata integra l'appliance FortiGate con altri fattori di sicurezza, come firewall virtuali, firewall cloud-native e Firewall-as-a-Service, per realizzare una soluzione HMF perfetta in tutto l'ambiente IT. I più recenti FortiGuard AI-Powered Security Services assicurano difese aggiornate anche dagli attacchi più recenti ed avanzati.

[1] "HTTPS encryption on the web", Google Transparency Report, Google, visitato il 15 maggio 2023.

[2] Maria Korolov, "Network Encryption: A Double-edged Sword for Cybersecurity", Datacenter Knowledge, 8 marzo 2023.

[3] "Fortinet FortiGate 600F", Enterprise Firewall, CyberRatings.org, Q2 2023.

FORTINET

www.fortinet.com

giugno 28, 2023 12:33 PM
1711466-A-0-IT