SOLUTION BRIEF

Umfassende Transparenz über Anwendungen, Benutzer und Geräte mit FortiGate Next-Generation Firewalls

Zusammenfassung

Herkömmliche Firewalls können Verbindungen oft nur auf Port- und Protokollebene zulassen oder blockieren. Für heutige Anforderungen ist das zu wenig: Moderne Unternehmensnetzwerke – die von On-Prem-Rechenzentren bis hin zu Public Clouds, Niederlassungen und Firmengeländen auch Remote-Standorte und Homeoffices umfassen – brauchen einen Zugang, der dynamisch, kontextabhängig und nach dem Zero-Trust-Prinzip geregelt wird. Nur dann erhalten IT-Teams die nötige Transparenz über Anwendungen, Benutzer und Geräte, um Unternehmensnetzwerke in ihrer gesamten Weitläufigkeit wirksam vor Cyberbedrohungen zu schützen. Diese umfassende Sichtbarkeit aller Netzwerkelemente ist jedoch oft nicht vorhanden.

Über 95 % des Internetverkehrs ist mittlerweile verschlüsselt.[1]

Das Problem mangelnder Transparenz verschärft sich noch durch die fast durchgängige Verschlüsselung des Internetverkehrs. Stellen Unternehmen dann von teuren Hub-and-Spoke-Architekturen auf dezentrale Netzwerke mit direktem Internetzugang für Standorte um, entsteht eine massive Intransparenz. Böswillige Akteure können diese „toten Winkel" im Netzwerk, in die Security-Teams keine Einsicht haben, ausnutzen und Bedrohungen im verschlüsselten Datenverkehr in das Unternehmen einschleusen.

FortiGate Next-Generation Firewalls (NGFW) schließen diese Sicherheitslücken und bieten die dringend notwendige Transparenz über den verschlüsselten Datenverkehr sowie über Benutzer-, Anwendungs- und Geräteaktivitäten. Unternehmen können so kontextbezogene Netzwerk- und Sicherheitsrichtlinien erstellen und kontinuierlich anpassen, damit die digitale Transformation ein sicherer Erfolg wird. Als Kernkomponente einer Hybrid-Mesh-Firewall-Lösung (HMF) identifizieren und kontrollieren FortiGate NGFWs mit fortschrittlichen Datenerfassungs- und Analysetechnologien alle Benutzer, Anwendungen und Geräte im Netzwerk und integrieren diese Transparenz und Security einheitlich in sämtliche IT-Bereiche. So wird ein starker, umfassender Schutz für die gesamte Netzwerkinfrastruktur erreicht.

Application Control

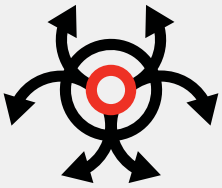
Der FortiGuard Application Control Service stellt eine Verbindung zu FortiGate NGFWs her und identifiziert schnell bekannte sowie unbekannte Anwendungen im Netzwerk. Dieser Dienst ermöglicht die einfache Festlegung von Richtlinien, die den Zugriff auf Anwendungen, bestimmte Funktionen innerhalb von Anwendungen und Anwendungskategorien erlauben, verweigern oder einschränken.

Nr.	Risiko	Anwendungen	Kategorie	Technologie	Benutzer	Bandbreite	Sitzungen
1	5	Asprox.Botnet	Botnet	Client-Server	1	1.74 MB	587
2	5	Proxy.HTTP	Proxy	Netzwerk-Protokoll	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

FortiGate NGFWs können Anwendungen nicht nur durch einen Port- und Protokollabgleich erkennen, sondern auch anhand der Anwendungssignatur, heuristischer Verhaltensweisen und anderer Identifizierungsindikatoren. Durch die kombinierte Analyse von Anwendungssignaturen und ISDB-Anwendungen (Internet Service Database) kann eine FortiGate über 4200 Application-Control-Regeln umsetzen. Im Folgenden finden Sie einige FortiGate-Funktionen für die Anwendungserkennung, die über den Layer 3 und 4 hinausgehen:

Anwendungssignaturen: Zulässigem Netzwerkverkehr wird eine Signatur zugewiesen, die auf den Transaktionsmerkmalen und dem von der Anwendung verwendeten Port basiert (Standard-Port oder unüblicher Port). Der Datenverkehr wird so auf Bedrohungen gescannt und eingehend analysiert.

Verschlüsselung: Erkennt die FortiGate eine Verschlüsselung – wie SSL/TLS (Secure Sockets Layer/Transport Layer Security), HTTPS (Hypertext Transfer Protocol Secure) oder SSH (Secure Shell) – und es gibt eine Richtlinienregel für die Entschlüsselung, wird die Sitzung entschlüsselt und die Anwendungssignaturen werden erneut auf den entschlüsselten Datenfluss angewendet.



„… bei Unternehmen mit einer Überprüfung des eingehenden Datenverkehrs kamen 70 % der Malware über verschlüsselte Verbindungen herein.“[2]

Decoder: Ist das Anwendungsprotokoll bekannt, werden zusätzliche kontextbasierte Signaturen angewendet. Diese können weitere Anwendungen erkennen, die womöglich im Protokoll versteckt sind (Tunneling). Die Decoder überprüfen, ob der Datenverkehr mit der Protokollspezifikation übereinstimmt, unterstützen die NAT-Traversal (Network Address Translation) und öffnen dynamische Durchlässe (Pinholes) für Anwendungen wie SIP (Session Initiation Protocol) oder FTP (File Transfer Protocol).

Heuristik: Die heuristische Analyse der FortiGate identifiziert schwer zu erfassende Anwendungen mithilfe von Verhaltensanalysen. Das können z. B. Anwendungen ein, die den Port 80 oder 443 verwenden oder zwischen mehreren Ports wechseln (Port Hopping). Letzteres ist oft bei VoIP-, Collaboration- und P2P-Anwendungen (Peer-to-Peer) der Fall, die selbst durch erweiterte Signatur- und Protokollanalysen nicht identifizierbar sind.

Kann die FortiGate eine Anwendung nicht anhand ihrer Signatur identifizieren, greift sie mittels Heuristik auf Verhaltensmerkmale zurück, ordnet die Anwendung einer bestehenden Anwendungsgruppe zu und wendet dynamische Filter oder eine richtlinienbasierte Weiterleitung an.

Die Identifizierung von Anwendungen bietet auch hilfreiche Kontextinformationen über das Netzwerk. So liefert die FortiGate z. B. Informationen über die inhärente Funktion, die Application-Ports, das Protokoll, die Technologie und die Verhaltenseigenschaften der Anwendung. IT-Teams können auf dieser Grundlage sichere, fundierte Zugangsrichtlinien festlegen. Ist nämlich ersichtlich, wie eine Anwendung im Netzwerk verwendet wird, lassen sich unterschiedlichste Richtlinien und Reaktionen anwenden, die über ein simples Zulassen oder Blockieren hinausgehen.

Mit der FortiGuard Application Control können Unternehmen außerdem Richtlinien erstellen sowie Funktionen innerhalb jeder Anwendung steuern, wie z. B.:

- Zulassen des Zugriffs auf Facebook, aber Blockieren von Dateiübertragungen über den Facebook Messenger
- Zulassen des Zugriffs auf Google Mail, aber Deaktivieren von Google Chat
- Blockieren von Datei-Uploads auf Dropbox, Box oder Google Drive
- Filtern von unerwünschten Videokategorien, die auf YouTube nicht angesehen werden sollen

FortiOS (das Betriebssystem der FortiGate) bietet mit Ansichten, Visualisierungen und Berichten einen umfassenden Echtzeit-Einblick in die Anwendungsnutzung und in Trends im Zeitverlauf. Die Application Control blockiert außerdem bösartige, riskante und unerwünschte Anwendungen durch Kontrollpunkte am Netzwerkrand, im Rechenzentrum sowie intern zwischen Netzwerksegmenten.

Benutzeridentifizierung

Die Erkennung von Benutzern über ihre IP-Adressen hinaus ist ein weiterer wichtiger Bestandteil der Security für Unternehmen. FortiOS kann Benutzer anhand unterschiedlichster Quellen und Methoden identifizieren, z. B. Microsoft Active Directory (AD), LDAP-Server, Syslog, Port-Mapping oder XFF-Header.

Die FortiGate-Benutzeridentifizierung bietet einen besseren Einblick in Netzwerkaktivitäten zur Erkennung von bösartigem oder schädlichem Verhalten. Anwender werden an jedem beliebigen Standort identifiziert – unabhängig vom Betriebssystem. Die Anwendungsnutzung durch Benutzer wird somit transparent und IT-Teams erhalten eine aussagekräftigere Übersicht über die Netzwerkaktivität.

Wie leistungsfähig die Benutzeridentifizierung ist, zeigt sich, wenn eine unbekannte Anwendung im Netzwerk gefunden wird. Mit FortiView sowie in den Application-Control-Logs können Security-Teams Folgendes erkennen:

- die Anwendung
- den Benutzer
- die Bandbreite und den Speicherverbrauch der Session
- Quelle und Ziel des Anwendungsverkehrs
- alle damit einhergehenden Bedrohungen

Benutzerzuordnung

Die FortiGate kann Profile von Benutzern im Netzwerk erstellen und Benutzernamen mit den IP-Adressen in empfangenen Paketen abgleichen. Benutzerinformationen können Sicherheitsrichtlinien zugeordnet werden, um die Netzwerknutzung sicherer zu gestalten. Zudem lässt sich der Zugriff auf eine Anwendung auf die Benutzer begrenzen, die diese unbedingt für ihre Arbeit brauchen. Mit der Benutzerzuordnung kann außerdem ein Regel- oder Richtliniensatz für weniger riskante Anwendungen (wie Salesforce oder PowerPoint) festgelegt werden, während gleichzeitig strengere Richtlinien für sensible Anwendungen wie Pen-Test-Tools oder Remote-Desktop-Controller gelten.

Gruppenzuordnung

Die Definition von Richtlinienregeln für Benutzergruppen vereinfacht das IT-Management: Wird ein Benutzer zu einer Gruppe hinzugefügt, gelten automatisch die vorhandenen Richtlinien und Regeln für diese Gruppe – nichts muss neu konfiguriert werden. Durch Anwendung und Aktualisierung der Regeln für eine ganze Gruppe kann die FortiGate auch unterschiedlichste Directory-Server unterstützen, wie Microsoft AD, Novell eDirectory oder Sun ONE Directory Server. Zusätzlich lassen sich weitere Sicherheitsrichtlinien für bestimmte Benutzer und Gruppen konfigurieren (z. B. für Anwendungskategorien und -unterkategorien, zugrunde liegende Technologien oder Anwendungsmerkmale) sowie Richtlinienregeln darüber, welche Anwendungen für welche Benutzer oder Benutzergruppen in welche Richtung (aus- oder eingehender Datenverkehr) verfügbar sind.

Beispiele für benutzerbasierte und gruppenbasierte Richtlinien:

- Tools wie SSH, Telnet und FTP auf Standard-Ports darf nur das IT-Team verwenden.
- Richtlinien wie:
  - Vertrieb/Verkauf darf auf Salesforce und Microsoft 365 zugreifen.
  - Alle Benutzer dürfen auf YouTube zugreifen, aber bestimmte Videokategorien sind gesperrt.

Die Benutzeridentifizierung hilft bei der Gestaltung von Richtlinien, die Mitarbeiter, Gäste und andere Interessengruppen unterstützen und schützen. Die FortiGate liefert nicht nur umfassende Insights über Benutzer, sondern kann auch Richtlinienkontrollen automatisieren.

Geräteidentifizierung

Hiermit lassen sich Richtlinienregeln für Geräte festlegen – unabhängig von Änderungen an der IP-Adresse oder dem Gerätestandort. Durch die Rückverfolgbarkeit von Geräten und die Zuordnung von Netzwerkereignissen zu bestimmten Geräten liefert die Geräte-ID den Kontext, welche Geräte bei diesen Ereignissen wie involviert waren. Diese Richtlinien sind explizit Geräten zugeordnet, statt Benutzern, Standorten oder IP-Adressen, die sich ändern können. Die Geräte-ID ist wichtig für Sicherheits-, Entschlüsselungs-, QoS- und Authentifizierungsrichtlinien.

Mit der FortiGate lassen sich erweiterte Geräterichtlinien und Prioritäten kategorisieren nach:

- Klasse wie sichere Geräte im Netzwerk
- kritischen Geräten wie Server oder Medizintechnik
- Umgebungsgeräte wie Ausweisleser, Kameras oder Feuermelder
- IoT-Geräte (Internet der Dinge) wie Smartwatches und andere verbundene „intelligente“ Geräte

SSL/TLS-1.3-Entschlüsselung

Da Malware oft im verschlüsselten Datenverkehr eingeschleust wird, muss dieser Traffic unbedingt überprüft werden. Ein Vorteil der FortiGate NGFWs ist, dass ihre SSL/TLS-1.3-Entschlüsselung das Netzwerk nicht ausbremst. Dank der leistungsstarken, proprietären Sicherheitsprozessoren von Fortinet geht der Firewall-Schutz nie zu Lasten der Netzwerkleistung. Ein weiterer Vorteil ist, dass sich mit einer FortiGate auch nur gewisse Arten von Datenverkehr entschlüsseln und z. B. Websites oder bestimmte Kategorien ausschließen lassen.

Zentrales, einheitliches Management

Dies ist eine der wichtigsten Funktion einer Hybrid-Mesh-Firewall (HMF). Müssen IT-Teams für den Schutz getrennter Bereiche – wie Unternehmensstandorte, Public Clouds, Private Clouds und Remote-Mitarbeiter – separate Dashboards im Blick behalten, steigt die IT-Komplexität und die Transparenz nimmt ab.

Ein zentrales Management koordiniert und vereinheitlicht unterschiedliche Sicherheitsbereiche zu einer einzigen IT-Security für Unternehmen. Das Ergebnis ist ein unkomplizierter, einheitlicher und automatisierter Schutz, der alle Unternehmensstandorte bis hin zur Cloud und zu Remote-Mitarbeitern sichert. Wichtig dabei: Da jedes Unternehmen andere Anforderungen an das Management dezentraler Netzwerk-Firewalls hat, müssen sämtliche Formfaktoren unterstützt werden – einschließlich Appliances, VMs, SaaS und Managed Firewall Services.

Ein zentrales Management bietet zudem einen hohen Zusatznutzen für die Zusammenarbeit des Network Operations Center (NOC) und Security Operations Center (SOC): Damit lassen sich Netzwerk- und Security-Teams zusammenbringen, um gemeinsam über eine einzige „Schaltzentrale" die gesamte Angriffsfläche zu verwalten, zu überwachen und zu schützen.

FortiGuard KI-gestützte Security-Dienste

FortiGate NGFWs bieten einen stets aktuellen Schutz für das gesamte Netzwerk in Echtzeit. Dafür verwenden die FortiGates die neuesten globalen Bedrohungsinformationen, die weltweit mit über 8 Millionen Sensoren erfasst und über die KI-gestützten FortiGuard Security-Dienste bereitgestellt werden. FortiGates schützen das gesamte Netzwerk mit mehrstufigen Sicherheitsmaßnahmen wie URL- und DNS-Filter, Anti-Malware, Inline-Sandboxing, einer hardwarebeschleunigten Abwehr von illegalen Zugriffen (Intrusion Prevention System, IPS) und einem leistungsstarken, virtuellen Patching. Diese Cybersecurity-Services bieten Sicherheit vor bekannten und noch unbekannten Angriffen. Unabhängige Tests von CyberRatings.org[3] attestieren der FortiGate NGFWs eine Wirksamkeit von 99,88 % bei der Abwehr bösartiger Angriffe und versuchter Umgehungen von Sicherheitsmaßnahmen.

Fazit

Die Identifizierung von Anwendungen, Benutzern und Geräten im Netzwerk ist eine unverzichtbare Funktion beim Management und Schutz von Unternehmensnetzwerken. FortiGate NGFWs sind für ihre erweiterte Transparenz und Kontrolle über den Netzwerkverkehr sowie ihre beispiellose Leistung bekannt. Mit einer FortiGate können Unternehmen angemessene Nutzungsrichtlinien definieren und automatisieren, Bedrohungen abwehren und ihre Angriffsfläche verringern. Dank dem zentralen, einheitlichen Management lässt sich die FortiGate-Appliance mit Sicherheitslösungen in anderen Formfaktoren – wie virtuellen Firewalls, cloudnativen Firewalls und Firewall-as-a-Service – leicht integrieren, um eine nahtlose HMF-Lösung für die gesamte IT-Umgebung zu schaffen. Zusätzlich sorgen die neuesten Bedrohungsinformationen, bereitgestellt über die KI-gestützten FortiGuard Security-Dienste, für einen aktuellen Echtzeit-Schutz vor selbst den neuesten und hochkomplexesten Angriffen.

[1] „HTTPS encryption on the web". Google Transparency Report, Google, abgerufen am 15. Mai 2023.

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

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

FORTINET

www.fortinet.com/de

28. Juni 2023
1711466-A-0-DE