SOLUTION BRIEF

Netzwerk-Management für die Fortinet Security Fabric automatisieren

Zusammenfassung

Durch die rasche Einführung digitaler Innovationen sind Netzwerke und die Netzwerk-Security wesentlich komplexer geworden – und auch anfälliger. Bösartige Cyber-Angriffe sind weiterhin ein ernstes Problem. Allerdings gingen im Vorjahr 48 % der Sicherheitsvorfälle auf harmlose Ursachen zurück und wären vermeidbar gewesen.[1] Zudem werden 75 % der Netzwerk-Ausfälle und Performance-Probleme durch Fehlkonfigurationen verursacht.[2] Eine Netzwerk-Security-Strategie mit Priorität auf Automatisierungen kann daher entscheidend dazu beitragen, eine der Hauptursachen für Cyber-Risiken und Ausfallzeiten zu reduzieren: menschliche Fehler und falsche Konfigurationen.

Das Fortinet Fabric Management Center – bestehend aus dem FortiManager und FortiAnalyzer – ist ein wichtiger Bestandteil der Security Fabric und vereinfacht den Netzwerk-Betrieb. Netzwerk-Infrastrukturteams in Unternehmen jeder Größe erhalten damit eine Lösung, um diese zentralen Herausforderungen anzugehen.

Wichtige Anwendungsfälle für das Fortinet Fabric Management Center:

- Zentrales Management
- Netzwerk-Automatisierung und Orchestrierung
- Security Fabric Analytics

Komplexität des Netzwerk-Betriebs

Zunehmend komplexe – und dadurch fragmentiertere – Infrastrukturen begünstigen die Zunahme von Cyber-Ereignissen und Netzwerk-Ausfällen. In den meisten Unternehmen sind zu viele isolierte Einzelprodukte installiert, von denen jedes mit einer eigenen Management-Konsole verwaltet werden muss. Auch Möglichkeiten zur Automatisierung sind meistens nur auf ein einziges Produkt beschränkt. Infolgedessen fehlt vielen Netzwerk-Operations-Teams ein umfassender, einheitlicher Einblick in die Einstellungen und Konfigurationen innerhalb der gesamten Infrastruktur – ganz zu schweigen von einer transparenten Netzwerk-Übersicht zur Erkennung von Anomalien.

Mit einer integrierten Netzwerk-Security-Architektur mit Automatisierungsfunktionen können Netzwerk-Betreiber komplexitätsbedingte Probleme leicht beseitigen. Durch die Kombination von FortiManager und FortiAnalyzer erhalten Unternehmen mit dem Fortinet Fabric Management Center drei Grundelemente für einen effektiven Netzwerk-Betrieb:

- Zentrales Management
- Netzwerk-Automatisierung und Orchestrierung
- Security Fabric Analytics

Zentrales Management

Isolierte Einzelprodukte für die Netzwerk-Security können in der Regel keine Bedrohungsdaten austauschen oder eine koordinierte Abwehrreaktion unterstützen. Dieses Defizit bei der Cyber-Sicherheit wird noch durch den Fachkräftemangel im Sicherheitssektor verschärft: Es fehlen schlichtweg die Mitarbeiter, um die Fülle an unterschiedlichen Produkten richtig zu konfigurieren und einzusetzen. Aber auch große Unternehmen mit eigenen IT-Security-Teams haben Probleme mit dem Netzwerk-Monitoring und können oft nur schwer feststellen, welche Geräte mit dem Netzwerk verbunden sind, wer Zugriff auf das Netzwerk hat und welche Ressourcen von welchen Anwendungen und Workflows benötigt werden.

Eine zentrale Management-Lösung mit einer einheitlichen, umfassenden Übersicht wie das Fabric Management Center schafft eine optimale Transparenz, die die Komplexität reduziert. Netzwerk-Operations-Teams können hiermit Datenbewegungen überwachen und anomale Aktivitäten erkennen. Auch vereinfacht eine solche „Schaltzentrale“ die Optimierung der Sicherheitslösung und fasst das Management von Next-Generation-Firewalls (NGFW) und anderen Security-Tools zusammen. Zudem lassen sich Betriebsabläufe für personell begrenzte oder unterbesetzte IT-Teams optimieren, was wiederum Arbeitsstunden spart und die Gesamtbetriebskosten (TCO) senkt.

Abbildung 1: Fortinet Fabric Management Center

Umfassendes Geräte-Management:

- Zentrale Verwaltung von NGFWs, SD-WAN (Software Defined Wired Area Network), SD-Branch (Software Defined Branch) und anderen Anwendungsfällen mit einer einzigen Konsole
- Für mehr als 100 000 Fortinet-Geräte skalierbar

Unternehmenskonfiguration und Change-Management:

- Geografisch dezentrale Hochverfügbarkeit mit bis zu fünf Einheiten
- Administrative Domains zur besseren Trennung von Netzwerken (Segregation)

Transparenz:

- Erweitertes Reporting und Dashboards für Operations und Security
- Planungs-Tools für Berichte

Netzwerk-Automatisierung und Orchestrierung

Insbesondere Unternehmen mit komplexen Infrastrukturen treiben die Implementierung von Automatisierung und Orchestrierung voran. Angestrebt wird eine Konsolidierung des Konfigurations- und Change-Management von komplexen, hybriden Netzwerken – übergreifend über NGFWs, SD-WANs und viele andere Anwendungsfälle. Dies geschieht vor allem aus Sicherheitsgründen.

Operations-Teams müssen aktiv auf Anomalien achten, da immer mehr Unternehmen auf Homeoffices umstellen. Auch müssen Unregelmäßigkeiten beim VPN-Zugriff (Virtual Private Network) in Echtzeit erkannt werden können. Dies ist jedoch nicht machbar, wenn vorhandene Tools weder integriert noch automatisiert sind. Das Fabric Management Center ermöglicht die Automatisierung und Orchestrierung komplexer Infrastrukturen mit Konnektoren, Automation-Hooks und Echtzeit-Warnungen bei Netzwerk-Anomalien.

Abbildung 2: Dashboard für die Automatisierung und Orchestrierung im Fabric Management Center

Implementierung und Wartung:

- Offene API für das Management von Fortinet-Implementierungen und zur Integration mit externen Systemen für Bereitstellung, Monitoring, Inventory- und Change-Management
- CLI-Unterstützung (Befehlszeilen-Schnittstelle) mit Script-Beispielen

Netzwerk-Integrationen:

- Fortinet Fabric Connectors für die Integration eines zentralen, plattformübergreifenden Richtlinien-Managements, z. B. für SDNs (Software Defined Network), Clouds und Technologien anderer Anbieter
- Fortinet-Verteilerdienst, der als Upgrade- und Threat-Intelligence-Gateway für alle bereitgestellten Fortinet-Geräte fungiert

Workflow und Orchestrierung:

- Schnelle, automatisierte Reaktion mit FortiOS Automation Stitches – eine einfache Möglichkeit, um Aktionen bei bestimmten Bedingungen auszulösen
- Interoperabilität mit vorhandenen Management- und Analytics-Tools

Security Fabric Analytics

Ein transparenter Überblick über das gesamte Netzwerk lässt sich oft nur schwer erreichen – insbesondere, wenn Unternehmen zu einer ohnehin schon komplexen Infrastruktur weitere isolierte Einzellösungen hinzufügen. Wenn Netzwerk-Teams diese Einzelprodukte konsolidieren und die Vorteile von FortiOS für die Intrusion Prevention (IPS), VPNs, NGFWs, das SD-WAN, SD-Branch und andere Funktionen nutzen, lassen sich Telemetriedaten problemlos zwischen allen Implementierungen austauschen und Anomalien transparent in Echtzeit aufzeigen.

Mit dem FortiAnalyzer als Teil des Fabric Management Centers erhalten Unternehmen aktuelle Bedrohungsdaten von den FortiGuard Labs und können so Probleme in Echtzeit erkennen. Der FortiAnalyzer umfasst eine integrierte Analyse-Engine, die die Korrelation der Bedrohungsdaten für die gesamte Security-Infrastruktur erheblich vereinfacht: Anomalien werden anhand von Risikobewertungen priorisiert und die Ergebnisse der Bewertung dann für die gesamte Infrastruktur bereitgestellt. Das Management dieser zentralen Analytik-Funktionen erfolgt über die einheitliche Konsolenansicht des FortiManagers.

Die Analyse-Engine unterstützt auch eine Echtzeit-Visualisierung der Security Fabric. Mithilfe dieser Visualisierungen können Operation-Teams Risiken für das Netzwerk in Echtzeit identifizieren und untersuchen. Der FortiAnalyzer verfügt zudem über integrierte, einfach anpassbare Dashboards und Berichte. Diese Funktionen umfassen über 700 Datensätze für ein einfaches Onboarding – erweiterte Abfragen, die für Reaktionen in Echtzeit optimiert sind.

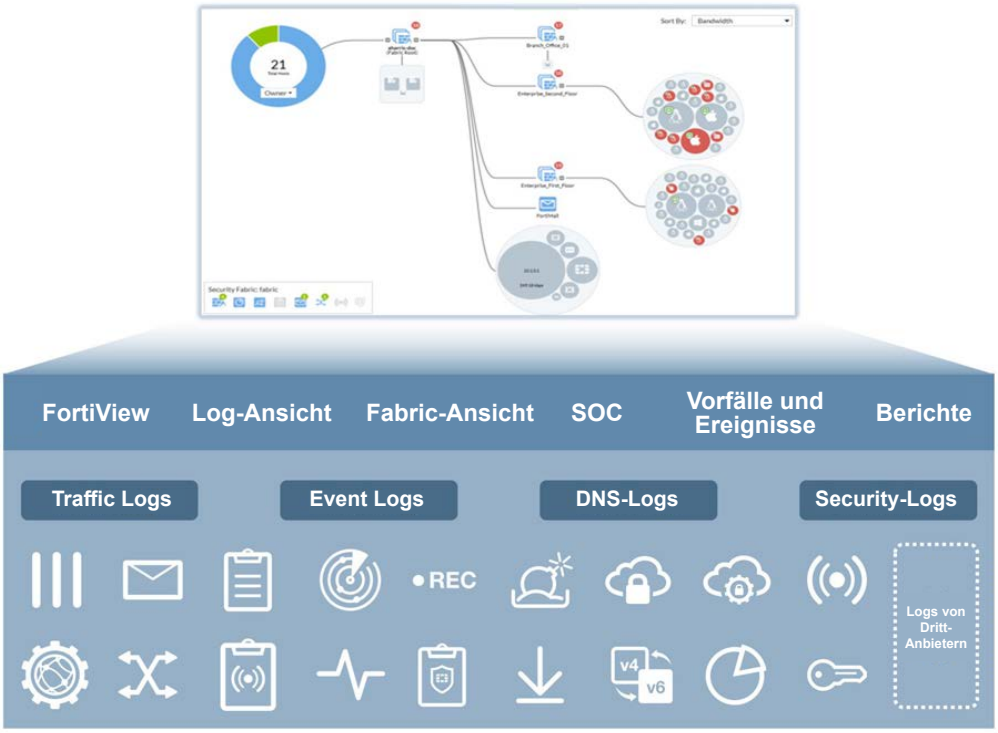

Abbildung 3: Analyseansicht im Fabric Management Center

Erweitertes Reporting:

- Unterstützung von Sicherheitsstandards wie NIST (National Institute of Standards and Technology) und CIS (Center for Internet Security)
- Einschließlich Security-Bewertung, basierend auf Hunderten von Security Best Practices von Fortinet

Rollenbasierte Transparenz:

- Spezielle Dashboards für Entscheidungsträger im Unternehmen wie CIOs, CISOs, Netzwerk- und Security-Architekten
- SecOps-Dashboard für Security-Teams mit Sicherheitsbewertungen

Security Fabric Backend:

- Integration in das FortiOS-Betriebssystem – kann für Topologien und andere Ansichten genutzt werden
- Verwendet Automation-Hooks von FortiAnalyzer und koordiniert Reaktionen in FortiOS

Stärkere Wertschöpfung aus der Security-Lösung im gesamten Unternehmen

Das Fortinet Fabric Management Center ermöglicht Sicherheitsfunktionen der Enterprise-Klasse und unterstützt Netzwerk-Verantwortliche bei der Realisierung branchenführender Vorteile:

Effizienzsteigerung: Mit seiner zentralen Ansicht vereinfacht der FortiManager die Überwachung der Security-Infrastruktur und ermöglicht eine automatisierte Reaktion auf potenzielle Probleme.

Risikominimierung: Die Tracking- und Reporting-Funktionen von Fortinet unterstützen Unternehmen bei der Einhaltung von Datenschutzgesetzen, Sicherheitsstandards und Branchenvorschriften. Gleichzeitig werden die mit Verstößen verbundenen Risiken von Bußgeldern und Rechtskosten reduziert. Der FortiAnalyzer verfolgt Bedrohungsaktivitäten in Echtzeit, erleichtert die Risikobewertung, erkennt potenzielle Probleme und wehrt Gefahren ab.

Geringere Gesamtbetriebskosten (TCO): Als Teil der Fortinet Security Fabric-Architektur trägt das Fabric Management Center zu geringeren Gesamtbetriebskosten bei, da bislang isolierte Security-Management-Funktionen konsolidiert werden. Mit dem FortiAnalyzer profitieren IT-Teams zudem von erweiterten Analyse- und Automatisierungsfunktionen, ohne dass teure Einzellösungen von Drittanbietern ergänzt werden müssen.

[1] „2019 Cost of a Data Breach Report“. Ponemon Institute und IBM Security, Juli 2019.

[2] Jeff Edwards: „Managing Network Configuration Changes: Five Best Practices“. WhatsUp Gold, 19. Juli 2018.

FORTINET

www.fortinet.com/de

31. August 2020, 8:43 Uhr

666918-0-1-DE