# Netzwerk-Firewalls

## „State of the Art“

CAIRO

secure • digital • IT-infrastructures

Netzwerk Firewalls sind inzwischen größere Systeme mit vielfältigen Aufgaben. Sie sind immanent wichtig für die Gefahrenabwehr und für den sicheren Netzwerkverkehr zwischen Systemen.
Der Markt der verschiedenen Hersteller ist seit 1990 im Fluss und es gibt jedes Jahr neue Technologien und Modelle - aber auch Preise/Kosten/Lizenzmodelle. Viele FWs, die aktuell im Einsatz sind, wie z.B. eine Sophos UTM gehen „out-of-support“ und es werden dringend Nachfolger gesucht.
Einige Firmen nutzen günstige Lösungen wie eine Sophos oder WatchGuard – andere nehmen Platzhirsche wie Fortinet oder Palo Alto. Aufgrund der Marktdominanz und wirtschaftlichen Entwicklung haben letztere – insbesondere Fortinet – ihr Portfolio auch in den unteren Leistungsklassen erweitert und nutzen ihre überlegende Technologie mit speziellen Sicherheits-Prozessoren auch in den günstigen Modellen.
Die folgenden Informationen geben einen Einblick in die aktuellen Herausforderungen & Lösungsmöglichkeiten.

## Aufgaben und Funktionsweisen einer FW oder Web App FW

Eine Firewall verhindert die Störungen oder das Eindringen eines Angreifers über verschiedene Attacken-Arten, regelt aber auch den Netzwerkverkehr nach außen mit z.B. einem Content-Filter. Sie ist **das** zentrale Element im Netzwerk und ist verbunden zum einen mit den Internet-Leitungen und zum anderen mit den - typischerweise Layer-3 - Switchen im LAN/VLAN und zu den Access Points/WLAN Router.

Faktisch arbeitet die Firewall auf OSI-Level 3 (Netzwerk, Protokoll) und 4 (Transport) während ein Layer-3 Switch gem. seines Namens auf Layer 3 und Layer 2 arbeitet.

Die korrekten und sicheren Einstellungen aller Regeln basieren also auf der genauen Kenntnis der Applikationen und deren genutzten Protokollen oder generischer Zugriffe von außen mit VPN. Bei niedrigen Anforderungen und kleinen Netzen kann die FW auch DNS oder DHCP-Service-Aufgaben mit übernehmen.

Eine Web Applikation selbst muss prinzipiell via https (443) zugreifbar sein und zwar ohne VPN - also ist hier eine Web Application Firewall (WAF) nötig. Diese funktioniert anders als eine herkömmliche FW und kann sogar durch White-Listing von Applikationszugriffen geschützt werden – dann aber mit dem Nachteil der erzwungenen Anpassung nach Applikations-Releasewechsel. Moderne Firewalls arbeiten nicht nur mit statischen Regeln sondern erkennen Angriffe auch verhaltensbasiert.

## Auf was kommt es bei der Modellauswahl und im sicheren Betrieb an?

- **Erkennung** von Attacken und Abwehr (**Signatur**-Update-Frequenz und Signatur-Güte)
- **Web Content Filter** Einstellungen
- **Durchsatz** & L**astverteilung** in Abh. von CPU, RAM und Protokollen für versch. Anschlüsse
- Failover bei Leitungsausfall ins Internet
- Failover mit FW-Cluster
- **Anschlüssse** wie 1 GE oder 10 GE für 10 Gbit/s
- **Einfache Administration:**
  - VLAN: einfache Konfiguration bei homogenen Firewall- und Switch-Modellen
  - Access Points booten aus der Ferne bei homogenen Firewall- und AP-Modellen
- **Regelwerke:** Einstellung der Regelwerke, Dokumentation, Changelog
- **Speicherung von Logs** für Forensic und das Audit
- Monitoring und Alarmierung
- Cloud / Non-Cloud: Welche Daten gehen in oder kommen aus der Cloud
- Sicherheits-Support & Services für Angriffsmuster
- OS und HW-Support & Services: Update, Ersatz-Garantien

## Angrenzende Themen im Netzwerk

- VLAN-Konfiguration
- VPN und VPN-Clients
- Token als MFA für VPN-Zugriffe
- Layer-3- Switche
- Access Points
- Mail Sicherheit Appliances, auch iV zu M365 und Exchange Online

## Kurzer Vergleich

**Fortinet** besitzt ein breites, integriertes Portfolio verschiedener Sicherheitstechniken (FortiGate, FortiWeb, FortiAnalyzer, FortiClient, FortiToken, FortiMail, uvm.) und stellt alles als Appliance oder VM zur Verfügung. Ein von sehr vielen Benutzern wertgeschätzter Vorteil sind die schnellen internen Prozessoren einer FortiGate und die lokale Datenspeicherung ohne wichtige Daten in die Cloud zu transferieren!
Die KI-gestützten FortiGuard Security Bundles bieten eine umfassende und sorgfältig zusammengestellte Auswahl an Security Services zur Bekämpfung von bekannten, unbekannten, Zero-Day- und neu entstehenden KI-basierten Bedrohungen.
Die Web Content Filter Kategorien bei der FortiGate sind sehr reichhaltig und lassen sich bzgl. ihres Verhaltens extrem flexibel einstellen.

Eine **Sophos** UTM (oder die Sophos-Nachfolgemodelle) ist stattdessen ein zusammengestellter Software Stack auf eingekaufter Hardware – teilweise mit Auswertung der Daten in der Sophos-Cloud. Zudem ist die Produktpalette deutlich reduzierter. So bietet Sophos auch keine zu der Firewall passenden Layer-3 Switche an.

### Cyber-Attacken auf eine Firewall

Als zentrales Element der Sicherheit ist eine Firewall natürlich jede Minute Cyber-Attacken ausgesetzt. So gelang es chinesischen Hackern bei 81.000 Sophos Firewalls weltweit Exploits erfolgreich auszuführen…die Liste der CVEs im folgenden Link spricht eine deutliche Sprache:
https://thehackernews.com/2024/12/us-charges-chinese-hacker-for.html

## Migrationsaufwendungen

Wie jede Migration ist die Aufnahme des IST-Zustand der bestehenden Regeln und Design der neuen Regeln nötig. Bestehende Regelungen sind häufig historisch (ad-hoc) gewachsen und umfassen teilweise tausende einzelne Regeln, von denen viele obsolete sind. Daher sollte man bei der Migration einen Neuaufbau/Neudesign der Regelwerke in Kombination mit einem Re-Design des Netzwerks (z.B. auch dort die VLAN-Struktur) in Erwägung ziehen. Das CAIRO Konzept startet immer mit den Applikationen, deren Benutzern und deren Performance-Anforderungen und zieht sich dann durch bis auf die einzelnen Regeln.

### Unsere Beratung, Kauf, Implementierung & Service

CAIRO berät Sie bei der Produkt- und Modellauswahl zu einer neuen Firewall nach den obigen Kriterien mit dem Fokus auf Fortinet als Marktführer.
Unsere Spezialisten nehmen Ihre Anforderungen auf, wählen die passenden kostengünstigen Modelle und führen anschließend die Migration durch. Optional kann man anschließend die Firewall oder auch anderen Geräte auch rechts- und auditkonform durch CAIRO sicher betreiben lassen.

**Die Netzwerkberatung ist Teil unseres Beratungs-Portfolios für moderne Infrastrukturen bis Security- und Compliance-Prüfungen, über das Schwachstellen-Management & Security Awareness Trainings bis zum sicheren IT-Betrieb.**

**CAIRO ist VdS 10000 zertifiziert für ein Informationssicherheits-Management System (ISMS).**

CAIRO
secure · digital · IT-infrastructures

Tel.: +49 (0)621 86 75 10 Mail: info@cairo.ag Web: www.cairo.ag