

## UTM / Firewall Network Appliances

### Ein Perimeterschutz braucht mehr als eine Firewall



Fortigate 60C



Fortigate 110C



Fortigate 310B

Leittechnische Systeme enthalten eine Fülle von wertvollen und wichtigen Informationen, die mit der heutigen Zusammenführung von technischen Prozessen, Daten aus Produktion, Lager und anderen Bereichen für das gesamte Unternehmen zugänglich gemacht werden. Die Verbindung der Netzwerke birgt ein verstärktes Sicherheitsrisiko, sowohl für die technische IT, als auch für die Business-IT.

#### UTM/Firewall: Umfassender Perimeterschutz

Klassischer IT-Security-Ansatz ist der Einsatz einer Firewall als Perimeterschutz. Diese Maßnahme schützt die zu separierenden Netzwerke vor Bedrohungen. Des Weiteren können Remote-Zugriffe sicher verwaltet werden. Aufgrund der Besonderheiten von leittechnischen Systemumgebungen, reicht hier jedoch eine herkömmliche Perimeter-Firewall nicht aus. Für effektiveren Perimeterschutz innerhalb kritischer Infrastrukturen bietet Industrial Defender die Fortinet FortiGate Unified Thread Management (UTM) Produkte mit erweiterter Funktionalität an. Verschiedenste Sicherheitstechnologien, inklusive einem ganzheitlichen Security-Ansatz sind in einem einzigen Gerät vereint. Das UTM wird an der Peripherie des Leitsystems platziert, um den Datenverkehr zu und von Systemen dynamisch zu regulieren, um Viren und versuchtes Eindringen abzuwehren und um sichere Verbindungen zu autorisierten Benutzern zu bieten.

#### UTM Features - Highlights

##### Firewall

Firewalls können Datenflüsse durch Leitsystemperimeter dynamisch regulieren und verhindern manipulativen oder nicht autorisierten Datenfluss. Das UTM bietet eine zertifizierte Firewall mit einer intuitiv bedienbaren graphischen Oberfläche.

##### Virenschutz

Host-basierte Virenschutzprogramme können problematisch sein, was Ressourcennutzung, Updates und Kompatibilität betrifft. Der zentral aktualisierbare Netzwerk-Virenschutz des UTM stoppt Schadsoftware, bevor diese in leittechnische Umgebungen vordringt. Die Systemperformance und die vorhandenen Steuerungsanwendungen werden nicht beeinträchtigt bzw. gefährdet.

##### Intrusion Prevention

Würmer und anderer Malware können leittechnische Systemkomponenten manipulieren. Das UTM System zur Intrusion Prevention entdeckt und stoppt diese Gefahren, bevor sie die technischen Systeme erreichen. Hierdurch werden die Systemzuverlässigkeit und Systemverfügbarkeit erhöht.

##### Remote-Access-Authentifizierung

Für leittechnische Systeme werden oft Standardpasswörter oder anlagenweit bekannte Passwörter verwendet, im schlimmsten Falle auch gar keine. Das UTM bietet ein einfaches Verfahren zur Bereitstellung individueller Logins mit sicheren Passwörtern, ohne aufwändige Eingriffe an der bestehenden Infrastruktur vornehmen zu müssen.

##### VPN (Virtual Private Networking)

Das UTM ermöglicht eine sichere "virtuelle Verbindung" für standortübergreifend vernetzte oder Remote-Access Anwendungen. Das UTM bietet als Gateway Standardoptionen, beispielsweise IPSEC, PPTP, L2TP, DES, 3DES, AES und andere. Auch ist das UTM für den Gebrauch mit allen gängigen Formen der Benutzer-Authentifizierung konzipiert, beispielsweise LDAP, Radius oder ähnliche Datenbanken. Das UTM bietet nicht nur eine zertifizierte VPN-Technologie, sondern entfernt auch Schadsoftware aus dem VPN-Verkehr.

## Der Industrial Defender Unterschied

Eine ganzheitliche elektronische Sicherheitsperimeter-Lösung für die leittechnische Systemumgebung sollte:

- Einfach vom Betriebspersonal zu bedienen sein, ohne Hilfe von der IT-Abteilung zu benötigen
- In die leittechnische Überwachung integriert sein
- Zugriff auf Perimeter Access Points
- überwachen und protokollieren und Warnmeldungen bei nicht autorisierten Zugriffsversuchen auslösen
- Möglichkeiten für Protokollierung und Reporting bieten, zur Unterstützung bei Audits und zur einfacheren Erfüllung von Compliance-Anforderungen

## Der Industrial Defender Mehrwert

Industrial Defender hat die Fortinet Fortigate UTM / Firewall Netzwerkgeräte mit erweiterten Funktionalitäten in sein durchgängiges Security-Konzept integriert. Diese Lösung hat gegenüber anderen, nicht in dieser Tiefe integrierten Produkte bzw. nicht für leittechnische Umgebungen optimierten Komponenten, die folgenden wichtigen Vorteile:

- Strategische Lockdown-Level für Netzwerksegmentierungen ermöglichen es den Benutzern, mit vorkonfigurierten UTM Konfigurationen schnell auf mögliche Bedrohungen zu reagieren. UTM Konfigurationen können zentral von der SEM Konsole aus zu einem oder mehreren UTM's übertragen werden. Das Betriebspersonal braucht keine Anpassungen vorzunehmen.
- Benutzer können Konfigurationen mehrerer UTM Einheiten innerhalb kürzester Zeit zentral ändern, beispielsweise wenn ein Serviceprovider vorübergehend Remote-Zugriff benötigt. Ohne eine durchgängige Security-Integration muss der Benutzer jede einzelne Firewall ändern, was je nach Entfernung und Einsatzort einige Stunden in Anspruch nehmen kann.
- Die zentralisierte Verwaltung der UTM Einheiten ermöglicht den Benutzern die schnelle Anpassung und Verteilung von bereits verwendeten Regelpaketen.
- Zentrale Verwaltung der IDS- und IPS-Signaturen sowohl für UTM's als auch für die Industrial Defender Network Intrusion Detection Sensoren (NIDS) auf der SEM Konsole. Alle Perimeter-IPS- und leittechnische IDS-Signaturen werden von einem einzigen System aus verwaltet und verteilt.
- Die Kombination von kritischen Cyber Asset Geräte- und Ereignisdaten innerhalb der SEM Konsole erleichtert die Erstellung von Auditberichten nach nationalen und internationalen Normenanforderungen. Der Security-Verantwortliche hat nur ein System für alle Auditdaten, statt vieler verteilter Systeme und Datenformate.

## Hardwareübersicht

Merkmal	Fortigate 60C	Fortigate 110C	Fortigate 310B
Firewall Durchsatz	1 Gbps	500 Mbps	1 Gbps
10/100 Mb Ports	8	8	0
10/100/1000 Mb Ports	5	2	10 (optional 14)
Stromversorgung	100-240 V, 50-60 Hz, 1,5 Amp (max)	90-240 V, 50-60 Hz, 2,0 Amp (max)	90-240 V, 50-60 Hz, 8,0 Amp (max)
Stromverbrauch	16 W (durchschnittlich)	120 W (durchschnittlich)	120 W (durchschnittlich)
Maße (BxHxT)	216 x 37 x 148 mm	330 x 46 x 254 mm	432 x 45 x 320 mm
Gewicht	0,9 KG	2,7 KG	6,35 KG

### Umgebungsbedingungen

Betriebstemperatur 10° C bis 40° C;

Luftfeuchtigkeit zwischen 10 und 90%, nicht kondensierend

### Produktzertifizierungen

FCC Class A Part 15, UL/CUL, C t i ck, VCCI

## KORAMIS GmbH

Kompetenzzentrum

Automatisierungstechnik & IT-Sicherheit

Neumühler Weg 32.1

D - 66130 Saarbrücken-Güdingen

Tel. +49 (0)681 - 968 191 - 30

Fax +49 (0)681 - 968 191 - 930

## KORAMIS – Ihr Partner für IT-Security

Als innovatives Unternehmen adressiert KORAMIS seit 1985 die Prozess- und Versorgungsindustrie und bietet Lösungen und Tools im technischen Umfeld von kritischen Infrastrukturen an. Im Bereich IT-Security ist KORAMIS Partner von Industrial Defender und bietet von der Risiko-Analyse über Lösungsimplementierung bis zum Support komplette Sicherheitslösungen aus einer Hand.