ENBITCON
we know IT

Ha(c)ken Sie Ihre Sicherheit nicht mit dem Kauf ab!

*Konzentrieren Sie sich auf Ihr Kerngeschäft und lassen Sie Ihre bei der **EnBITCon** erworbene Firewall durch unsere Experten einrichten.*

Unsere Techniker sind durch die jeweiligen Hersteller ausgebildet und zertifiziert, so dass wir eine professionelle, vollumfängliche und reibungslose Konfiguration Ihrer Firewall gewährleisten können.

299 €* *netto zzgl. MwSt.*

Analysieren Ihrer Netzwerkinfrastruktur

Einrichtung & Konfiguration

Inbetriebnahme

In 4 einfachen Schritten zur sicheren Konfiguration

1. *Sie füllen das untenstehende Formular vollständig aus.*
2. *Wir werten Ihre Informationen aus und halten vor Beginn der Einrichtung noch einmal Rücksprache mit Ihnen. Im Anschluss beginnen wir mit der Konfiguration Ihrer Firewall.*
3. *Die vorkonfigurierte Appliance wird an Sie versendet. Mit der beiliegenden Anleitung binden Sie die Firewall im Handumdrehen in Ihr Unternehmensnetzwerk ein.*
4. *Ihr Unternehmen ist jetzt grundlegend geschützt. Auf Ihren Wunsch können unsere Techniker noch weitere Funktionen konfigurieren, welche Sie individuell auswählen können.*

Telefon: +49 228 - 33 88 89 - 0
info@enbitcon.de | www.enbitcon.de

* *Der angegebene Preis bezieht sich auf ein physikalisches System bzw. eine virtuelle Instanz*

ENBITCON
we know IT

1. Zugangsdaten zum Lizenzportal

Für weitere Infos einfach auf die Logos klicken. Sie werden dann auf die Website weitergeleitet.
Fortinet | https://support.fortinet.com • Sophos SG | https://myutm.sophos.com • Sophos XG | https://secure2.sophos.com/de-de/mysophos/login.aspx

1.1 Benutzername

1.2 Passwort

2. Grundeinstellungen der Firewall

2.1 Hostname *(bspw.: firewall.meinefirma.de)*

2.2 Stadt

2.3 Land

2.4 Gewünschte Zeitzone *(Standard GMT+1 Berlin)*

2.5 Gewünschte(r) NTP Server

3. Lokale Netzwerkeinstellungen der Firewall

3.1 Gewünschte IP Adresse für lokales Netzwerk

3.2 Gewünschte Subnetzmaske für lokales Netzwerk

3.3 VLAN-Tag

☐ Ja ☐ Nein

Telefon: +49 228 - 33 88 89 - 0
info@enbitcon.de | www.enbitcon.de

ENBITCON
we know IT

4. Verbindung ins Internet

Diese Daten werden durch Ihren Provider vorgegeben.

4.1 Art der Verbindung

- [x] DHCP
- [ ] PPPOE (erfordert Modem)
- [ ] Statische IP Adresskonfiguration

4.2 Gewünschter DNS Server

- [x] per DHCP vom Provider vergeben
- [ ] statisch

5. Nützliche Funktionen im lokalen Netzwerk

5.1 Soll die Firewall als DHCP Server fungieren?

- [ ] Ja
- [ ] Nein

5.2 Soll die Firewall als DNS Server/Relay fungieren?

- [ ] Ja
- [ ] Nein

5.3 Soll die Firewall als NTP Server/Relay fungieren?

- [x] Ja
- [ ] Nein

6. Freigegeben Dienste aus dem lokalen Netzwerk ins Internet

6. Freigegebene Dienste aus dem lokalen Netzwerk ins Internet

- [ ] DNS
- [ ] HTTP
- [ ] HTTPS
- [ ] FTP
- [ ] IMAP / IMAPS
- [ ] SMTP/SMTPS
- [ ] POP3/POP3S

7. Webdienste

7.1 Wenn Sie weitere Programme oder Dienste nutzen, welche auf eine Internetverbindung außerhalb der Standardports angewiesen sind, teilen Sie uns bitte die Anwendung, sowie idealerweise die benötigten Ports und Protokolle (TCP/UDP) mit.

Telefon: +49 228 - 33 88 89 - 0
info@enbitcon.de | www.enbitcon.de

ENBITCON
we know IT

8. Tiefergreifende Inspektion

8.1 Soll die Firewall SSL Pakete scannen und analysieren?

☐ Ja ☐ Nein

8.2 Soll Anti-Portscan aktiviert werden?

☐ Ja ☐ Nein

8.3 Soll Intrusion Prevention aktiviert werden?

☐ Ja ☐ Nein

9. Web Protection

9.1 Soll die Firewall als Webproxy fungieren?

☐ Ja ☐ Nein

10. Email Protection

10.1 Sollen Emails gescannt werden?

☐ Ja ☐ Nein

Bitte beachten Sie, dass es sich bei einem Scan der verschlüsselten Protokolle technisch um eine „Man-in-the-Middle" Attacke handelt. Sie erhalten von uns vor Auslieferung das sogenannte Stammzertifizierungsstellen-Zertifikat der Firewall, welches auf den Rechnern im internen Netzwerk in den Speicher der „vertrauenswürdigen Stammzertifizierungsstellen" importiert werden muss.

11. Sandboxing

11.1 Sollen unbekannte Dateien in die Sandbox zur weiteren Analyse übermittelt werden?

☐ Ja ☐ Nein