

leistungsbeschreibung|managed firewall services

version 2.1
april 2010

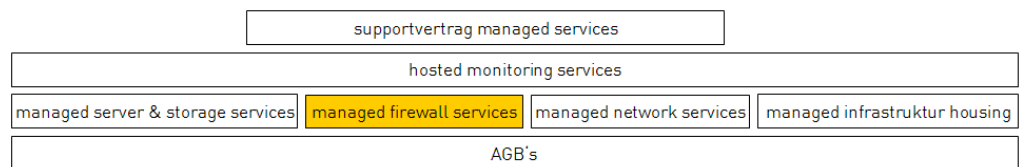
 **managed|firewall services**
by achermann consulting

Inhaltsverzeichnis

1 Managed Firewall Services	3
1.1 Ziel und Zweck	3
1.2 Nutzen für den Kunden	4
2 Dienstleistungen Firewall	5
2.1 Dienstleistungs-Matrix	5
3 Pflichten des Kunden	9
3.1 Voraussetzungen für Managed Firewall Services	9
4 Preise der Dienstleistungen	11
4.1 Preise für Managed Firewall Services	11
4.2 Preise für übergreifende Dienstleistungen	11
4.3 Kosten für Pikett Bereitschaftsdienst und Einsätze	12
4.4 Stundenansätze	13

1 | Managed Firewall Services

1.1 | Ziel und Zweck



Dieses Dokument beschreibt die Leistungen von **managed|**firewall services der **achermann consulting ag** (ac-ag). Die Leistungsbeschreibung enthält die Aufgaben, Verantwortung und Kosten der zu erbringenden Dienstleistungen.

managed|firewall services bedeutet, dass ac-ag die höchstmögliche Sicherheit sowie die mit dem Kunden definierten Verfügbarkeiten gewährleistet und somit die Verantwortung der Firewalls übernimmt, egal ob die Firewalls beim Kunden oder im ac-ag Datacenter stehen. In beiden Fällen übernimmt ac-ag für den Kunden sämtliche technische wie auch administrative Arbeiten.

Sämtliche allgemeinen vertraglichen Bedingungen wie Betriebs- und Reaktionszeiten, Vertragslaufzeit, Konditionen, Sorgfaltspflicht des Kunden, Haftbarkeiten und Schlussbestimmungen werden im **supportvertrag|**managed ict-services behandelt. Der Supportvertrag, sowie deren Anhänge, müssen durch den Kunden unterzeichnet werden.

1.2 | Nutzen für den Kunden

- **Kosten sparen:**
Einsparung von Investitionen im Bereich der Überwachungstools sowie der teuren Ausbildungskosten für eigene Firewall-, IT-Security- und Netzwerkspezialisten. Transparenz und Messbarkeit der genannten Dienstleistung und der Zusatzservices.
- **Ressourcen entlasten:**
Entlastung der internen IT-Ressourcen beim Kunden durch die zertifizierten ac-ag Firewall-, IT-Security- und Netzwerkspezialisten.
- **Kompetenter Telefonsupport:**
Zu den Bürozeiten ist für die ac-ag Managed ICT-Services Kunden der kompetente und persönliche Support eine Selbstverständlichkeit.
- **Proaktive Überwachung:**
Unser Überwachungssystem reagiert bei einer Störung sofort und leitet die Meldung per SMS oder E-mail an die ac-ag Supportorganisation weiter. Die Service Level Vereinbarung wird mit dem Kunden definiert und hinterlegt.
- **7x24h Pikettdienst:**
Unser 7x24h Notfalldienst ergänzt den Telefonsupport sowie Einsätze vor Ort ausserhalb der Bürozeiten. Die jeweiligen System-Engineers stellen den Pikettdienst ausserhalb der Bürozeiten.
- **Kontinuierliche, technische Sicherheitsüberprüfungen:**
Sicheres Aufzeichnen des Kunden Firewall SYSLOGS während 30 Tagen in der ac-ag SQL Datenbank. Aktualisieren der Subscription Software (Securityupdates) auf der Firewall.

Die Dienstleistung **managed|firewall services** garantiert dem Kunden keinen abschliessenden Schutz vor Bedrohungen und Angriffen aus dem Internet. Der Service garantiert dem Kunden auch keine Verfügbarkeiten der eigenen Informatikinfrastruktur und schützt diese auch nicht vor Viren und Trojanern.

Der Service **managed|firewall services** konzentriert sich auf das konstante Unterhalten und Überwachen des Internetzuganges zum LAN des Kunden. Die Leistungen der ac-ag sind im Kapitel 2.1 ausführlich beschrieben.

2 | Dienstleistungen Firewall

Das Kundenunternehmensnetzwerk (LAN) wird mit einer Box to Box VPN Verbindung (IP-Sec) permanent mit der ac-ag Management Infrastruktur verbunden. Dabei bildet die kundeneigene Juniper NetScreen Firewall die zentrale Komponente der Sicherheitslösung, egal ob die Firewalls beim Kunden vor Ort oder im Datacenter der ac-ag stehen. Das Management erfolgt immer zentral durch unsere ausgewiesenen Firewall-, IT-Security- und Netzwerkspezialisten in Luzern. Tritt ein Fehler oder Problem auf, garantieren wir eine schnelle und gezielte Reaktion. Das Supportteam sorgt auch für proaktive Überwachung und Unterhalt der Firewalls.

2.1 | Dienstleistungs-Matrix

In den folgenden Dienstleistungsbeschreibungen werden Massnahmen beschrieben, welche ac-ag erbringt, um möglichst hohe Grundstabilität der Firewall zu erreichen und somit Störungsausfälle zu vermindern. Treten Störungen auf, werden unsere Supporter via SMS oder E-Mail sofort darüber informiert.

Ausgeschlossen sind Störungen, Ausfälle oder Unterbrüche, die durch höhere Gewalt, Fehlmanipulation der Benutzer des Kunden oder Sabotage verursacht wurden. Zur Sabotage werden unter anderem auch Ereignisse wie zum Beispiel Hackerattacken oder Virenbefall gezählt. Die Behebung solcher Störungen, Ausfälle oder Unterbrüche werden zusätzlich nach Aufwand verrechnet.

Art-Nr.	Dienstleistungspositionen	Ausführung		Verrechnung
		Frequenz	Bemerkung	
Monitoring Solution				
MON-1	Standard Monitoring Service Überwachung mit Ping & SNMP Alarm erfolgt via E-mail & SMS	laufend		P (Standard)

Art-Nr.	Dienstleistungspositionen	Ausführung		Verrechnung
		Frequenz	Bemerkung	
Managed ICT-Services				
MFS	Regelmässige Juniper Subscription Updates einspielen. Diese werden durch Juniper Networks im jährlichen Abonnement zur Verfügung gestellt	quartalsweise	Patch Night	P (Standard)
	Unterhalt und Wartung der Policies und Regeln auf der unter Vertrag stehenden Juniper NetScreen Firewall	quartalsweise		P (Standard)
	Proaktive Überwachung der Security Settings (spezielle Auswertungen der Logfiles der Firewall auf den zentralen SYSLOG Managed Firewall SQL Datenbank bei ac-ag)	quartalsweise		P (Standard)
SEC-CH	Managed Security Check auf die externe Verletzbarkeit (Vulnerability) des Kunden	quartalsweise	quartalsweise	O (Optional)
Nach Aufwand	Security Monitoring: SYSLOG Analyse, um Schwachstellen im Netzwerk zu erkennen	Auftrag durch Kunde		O (Optional)

P = Pauschale (Dienstleistungen im Preis inbegriffen)

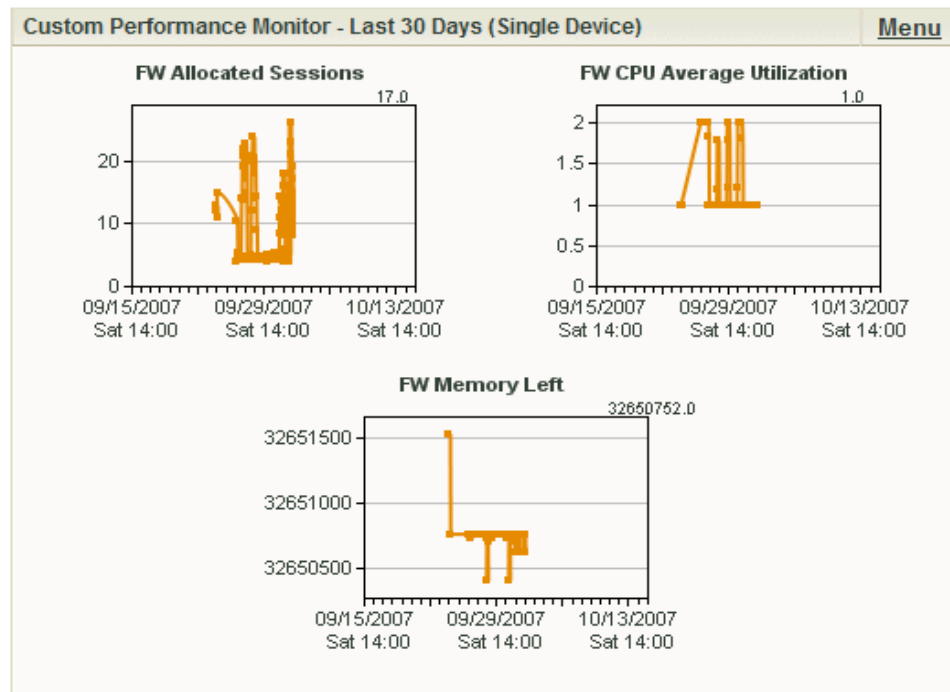
O = Zusatzoptionen werden analog Preistabelle verrechnet

2.1.1|Monitoring Solution

Standard Monitoring Service

Mit einem Ping wird die Verbindung überprüft und alle 60 Sekunden auf den Überwachungsmonitor übertragen. Sobald der Status von grün auf gelb und dann auf rot wechselt, wird automatisch eine Meldung generiert und an die zuständige ac-ag Supportorganisation weitergeleitet.

Folgende Parameter werden gemessen, aufgezeichnet und überwacht: CPU Auslastung, Memory Ressourcen, Session Handling und die Anzahl Policies auf der Firewall.



2.1.2|Standard Managed ICT-Services

Regelmässige Juniper Subscription Updates einspielen

BASIS-MFS

Durch den Erwerb der Juniper Subscription erhält der Kunde das Anrecht, die Firewall mit dem neusten Betriebssystem auszustatten. Die Updates werden durch die ac-ag in regelmässigen Abständen via Remotezugriff installiert. Sollte die Firewall einen technischen Defekt aufweisen, wird eine gleichwertige Firewall als Ersatz während der Reparaturzeit zur Verfügung gestellt.

Unterhalt und Wartung der Policies und Regeln

BASIS-MFS

Anhand der Regeln legt der Kunde fest, wie weit Anwendungen nach aussen aufgebaut werden dürfen. Tritt der Fall auf, dass aus irgendwelchen Gründen Anwendungen blockiert werden, muss dies durch den Kunden an die ac-ag Supportorganisation weitergeleitet werden. Ein zertifizierter Firewallspezialist der ac-ag wird die Firewallregeln via Remotezugriff ändern. Das ideale Regelwerk einer Firewall ist immer so aufgebaut, dass grundsätzlich jeder Netzwerk Verkehr verboten ist und die erwünschten Verbindungen erlaubt werden.

Proaktive Überwachung der Security Settings

BASIS-MFS

Sofern bei der Firewall die Antivirus Option freigeschalten ist, werden in regelmässigen Abständen die Antivirendefinitionen überprüft. Dies bedingt jedoch, dass diese Option zusätzlich lizenziert und durch die ac-ag freigeschalten wird. Zusätzlich werden die Logfiles der Firewall auf der zentralen SYSLOG Managed Firewall SQL Datenbank 30 Tage lang aufbewahrt. Das SYSLOG beinhaltet Meldungen der Kategorien: Emergency, Alert, Critical, Error und Warning. Sollten irgendwelche Störungen auftreten, können diese Logfiles durch unsere Firewallspezialisten untersucht werden.

2.1.3 Optional Managed ICT-Services

Managed Security Check

SEC-CH

Die Firewall wird auf externe Verletzbarkeit (Vulnerability) untersucht. Hier geht es darum, Schwachstellen ausfindig zu machen und zu entfernen. Dazu gehören, unerlaubten Zugang von VPN Tunnels und nicht autorisierten Benutzern zu überwachen, sowie offene Ports von nicht benutzten System- und Anwendungsdiensten zu untersuchen. Diese Gefahrenquellen sind nicht zu unterschätzen, da diese Sicherheitslücken Ziele von Hackern sind. Dieser Service wird quartalsweise durchgeführt.

Security Monitoring: SYSLOG Analyse

NACH AUFWAND

Sollten irgendwelche Anomalien im Netzwerk auftreten, kann der Kunde das SYSLOG auf interne und externe Probleme untersuchen lassen. Der Kunde erhält je nach Bedürfnis, detaillierte Berichte über Sicherheitsereignisse im Netzwerk.

3 | Pflichten des Kunden

Damit die ac-ag die in diesem Dokument festgehaltenen Dienstleistungen erbringen kann, müssen auch einige Pflichten durch den Kunden erbracht werden. Diese Voraussetzungen und Verpflichtungen sind ebenfalls Gegenstand des **supportvertrag** | managed ict-services.

3.1 | Voraussetzungen für Managed Firewall Services

Folgende Voraussetzungen müssen durch den Kunden (allenfalls zusammen mit der ac-ag) geschaffen werden, damit die Dienstleistung **managed** | firewall services durch ac-ag professionell erbracht werden kann:

- Permanenter Internetanschluss (ADSL oder xDSL Technologie) inkl. den notwendigen, öffentlichen IP-Adressen
- Das Jahresabonnement „Support Subskription“ muss beim Hersteller Juniper Networks abonniert sein (macht gegebenenfalls ac-ag für den Kunden)
- Bestehende Zugangsdaten, wie z. B. Passwörter zur Firewall, werden der ac-ag übergeben und der zur Installation und Wartung notwendige Zugang gewährt
- Die Firewall des Kunden wird mit der ac-ag Überwachungslösung (WhatsUp Gold) verschlüsselt verbunden, so dass die definierten Parameter permanent in die SQL DB übernommen, aufgezeichnet und ausgewertet werden können
- Der aktuelle Netzwerkplan der Infrastruktur wird zur Verfügung gestellt oder kann durch ac-ag nach Aufwand erstellt werden
- Ausbauten am Kundennetzwerk, welche die Konfiguration und Sicherheit der Firewall beeinträchtigen könnten, sind der ac-ag vorgängig mitzuteilen

Um die oben aufgeführten Leistungen erbringen zu können, muss eine Verbindung auf die Juniper NetScreen Firewall des Kunden hergestellt werden. Dieses verschlüsselte Einloggen auf die kundeneigene Firewall findet ausschliesslich über eine sichere Verbindung (SSL, SSH oder VPN) statt.

The screenshot displays the Juniper NetScreen-25 web management interface. The top navigation bar includes 'Home' and 'FWACAG01:NSRP(M)'. The main content area is divided into several sections:

- Device Information:**
 - Hardware Version: 4010(0)
 - Firmware Version: 5.2.0r2.0 (Firewall+VPN)
 - Serial Number: 0034042004000898
 - Host Name: FWACAG01
- System Status (Root):**
 - Administrator: (field)
 - Current Logins: 2 [Details](#)
- Resources Status:**
 - CPU:
 - Memory:
 - Sessions:
 - Policies:
- Interface link status:**

Name	Zone	Link
ethernet1	Untrust	Up
ethernet2	Trust	Up
- The most recent alarms:**

Date/Time	Level	Description
2007-03-22 08:42:12	crit	FIN but no ACK bit! From 71.105.91.159:3...
2007-03-22 08:11:42	crit	FIN but no ACK bit! From 71.105.91.159:3...
2007-03-22 07:46:09	crit	FIN but no ACK bit! From 71.105.91.159:4...
2007-03-22 06:45:40	crit	FIN but no ACK bit! From 71.105.91.159:4...
2007-03-22 05:38:37	crit	FIN but no ACK bit! From 71.105.91.159:3...
- The most recent events:**

Date/Time	Level	Description
2007-03-22 08:57:44	warn	Admin user " " logged in for Web(http...
2007-03-22 03:29:42	notif	The system clock was updated from primar...
2007-03-22 03:11:52	notif	VIP server is now alive.
2007-03-22 01:18:48	notif	VIP server is now alive.
2007-03-21 22:24:02	warn	Admin user "root" logged in for Web(http...

Abbildung 1: Beispiel der überwachten Parameter auf der Kunden Firewall

4| Preise der Dienstleistungen

4.1| Preise für Managed Firewall Services

Die Ausgangslage für jede einzelne Firewall ist das Basispaket BASIS-MFS. Je nach Bedürfnis können weitere Management Services hinzugefügt werden.

Geräte	Art-Nr.	Skalierbarkeit	*Preise pro Monat
Firewall	BASIS-MFS	- Standard Monitoring - Updates einspielen - Überwachung Device Settings	ab CHF 120.00
Firewall	MFS-AD	- Zusatzkosten grosse Firewall: Mehr User, Sessions, VPNS, V-LANs, etc.	bis CHF 230.00
Firewall	SEC-CH	- Managed Security Check	CHF 60.00
Voraussetzung		- Juniper – NetScreen Abonnement „Support Subscription“ Update	ab CHF 160.00/Jahr
Optional		- Managed Security Monitoring	Nach Aufwand
Optional		- Zusatzkosten für V-LAN, DMZ oder FDP Spezialkonfigurationen	Nach Aufwand zum ICT-Security Stundenansatz
Optional		- Ersatzgerät oder High Availability (HA) mit zweiter, redundant ausgelegter Firewall beim Kunden	50% der monatlichen Kosten

Im **supportvertrag** | managed ict-services werden die detaillierten Leistungen und Preise gemäss Kundenanforderungen individuell zusammengestellt. Als Basis dienen jeweils die im Anhang zum Supportvertrag aufgeführten Geräte des Kunden.

4.2| Preise für übergreifende Dienstleistungen

Zusatzkosten Monitoring Solution ac-ag		*Preise pro Monat
LOG	Kundeneigenes Login auf hosted monitoring services (Lizenzanteil)	CHF 50.00
MSA	hosted Secure Access Abo inkl. Token pro User	CHF 35.00

Mit diesen zusätzlichen Dienstleistungen kann der Kunde die abonnierten Services persönlich überwachen oder über einen geschützten Zugang selber verwalten. Weitere Details zum Produkt Managed Secure Access sind dem ac-ag Factsheet zu entnehmen.

4.3 | Kosten für Pikett Bereitschaftsdienst und Einsätze

Der ac-ag Pikett Bereitschaftsdienst (Abonnement) ist ein zusätzlicher ICT-Service für Supporteinsätze ausserhalb der regulären Betriebszeiten. Der Abonnementskunde hat somit während 7x24 Std. einen Zugriff auf die ICT-Supportorganisation der ac-ag für eine effiziente Störungsbehebung. Je nach Bedürfnis wählt der Kunde zwischen proaktiven und interaktiven Pikett Einsatz.

- Proaktiver Einsatz: Bei schwerwiegenden Störungen an den Kundensystemen wird der ac-ag Pikett Service über das ac-ag Überwachungssystem alarmiert und informiert. In der Service Level Vereinbarung (SLA) werden mit dem Kunden die Massnahmen der möglichen Ereignisse vorgängig definiert und im Pikett-Prozess des Kunden hinterlegt. Mit der proaktiven Überwachung wird ein Ausfall der Kundensysteme auf ein Minimum reduziert.
- Interaktiver Einsatz: Im Falle einer Störung entscheidet der Kunde über den Zeitpunkt des Einsatzes und kontaktiert, falls notwendig und Bedarf, den Pikett Service anhand des Kunden-Pikett-Codes per Telefon.
- Der Kunde bezahlt eine monatliche Bereitschaftsgebühr für den 7x24h Pikett Bereitschaftsdienst der ac-ag

7x24h Pikett Bereitschaft		*Preise pro Monat
PIK-1	proaktiver Einsatz (Bereitschaftspauschale)	ab CHF 300.00
PIK-2	interaktiver Einsatz (Bereitschaftspauschale)	ab CHF 200.00

- Wird der Pikettdienst, egal ob proaktiver oder interaktiver Einsatz, während den Pikettzeiten aufgeboden, sind die Pikett Grundgebühren von CHF 250.00 als Basiskosten geschuldet.
- Sämtliche Einsätze werden nach den ac-ag üblichen Tarifen und Zuschlägen gemäss Supportvertrag Kapitel 3 verrechnet.

4.4 | Stundenansätze

Dienstleistungen ausserhalb dieser Leistungsbeschreibung sowie einmalige Setup-
dienstleistungen werden nach Aufwand zu folgenden Stundenansätzen verrechnet:

Stundenansätze	*Preise pro Stunde
Ansatz für ac-ag ICT-Services Server & Storage (System Engineer)	CHF 180.00
Ansatz für ac-ag ICT-Services für Firewall & Netzwerk (Security- und Network Engineer)	CHF 200.00

Die Stundenabonnemente werden dem Kunden vor Erbringung der Supportleistungen in Rechnung gestellt, als Gutschrift ausgewiesen und stundenweise abgebucht. Folgende Ansätze zu den Fixstunden sind im Angebot:

Supportvertrag mit Stundenabonnemente		*Preise pro Stunde
D.01-50	Stunden Packet für Konfiguration & Installation (50 Std.)	CHF 170.00
D.01-100	Stunden Packet für Konfiguration & Installation (100 Std.)	CHF 160.00
D.01-200	Stunden Packet für Konfiguration & Installation (200 Std.)	CHF 150.00

*Alle aufgeführten Preise sind exkl. Mehrwertsteuer

Die monatlich wiederkehrenden Kosten verstehen sich für die in diesem Dokument definierten und durch ac-ag zu erbringenden Dienstleistungen. Die Abrechnung der **managed** firewall services erfolgt quartalsweise im Voraus.