

Firewall

Sensible Daten bedürfen einer soliden Absicherung. Deshalb bietet die *pegasus IT* mit der **Firewall** ein zuverlässiges Sicherheitskonzept für Ihren zentralen Übergangspunkt vom Unternehmen zum Internet. Dabei werden VPN-Verbindungen ebenso verlässlich unterstützt wie eine Vielzahl von Applikationsgateways. Mit einer **Firewall** schützen Sie Ihre IT-Infrastruktur gegen Angriffe aus dem Internet und minimieren damit verbundene Probleme wie z. B.

- Produktions- bzw. Systemausfälle
- Angriffe via Schadsoftware, Viren oder Würmer
- Verstöße gegen gesetzliche Vorschriften
- hohe Leitungsauslastung
- mangelnde Kontrolle über interne Netzwerke

Lösung /Produkt

Die **Firewall** ist flexibel an Ihre Bedürfnisse anpassbar: Diese kann sowohl auf Ihre WAN-Leitung als auch für einen redundanten Firewallcluster mit mehreren DMZ (Demilitarisierte Zonen) und Multiprovideranbindung individuell zugeschnitten und erweitert werden.

Folgende Leistungen sind enthalten:

- managed Firewall durch *pegasus IT*
- IDS / IPS zur Abwehr komplexer Angriffe aus dem Internet (optional)
- definierte Regelwerke für ein- und ausgehenden Datenverkehr
- Firewall-Softwareaktualisierung durch *pegasus IT*
- Ausfallsicherheit durch redundante HA-Firewalls bzw. Clusterkonzepten (High Availability, optional)
- Vollständige Integrierung in das Kunden MS Active Directory (Authentifizierung und Zugriffe)
- Bandbreitenmanagement, Quality of Service
- (Transparente) URL- und Applikationserkennung
- Implementierung von NIC-Bonding, VLAN-Trunks, DMZ,...
- Traffic Intelligence im VPN-Routing
- VPN / SSL-VPN
 - Antivirus
- URL-Filter
 - DNS/DHCP

pegasus IT ist zertifiziert nach DIN ISO/IEC 27001 im Bereich *Innovative Rechenzentrumsdienstleistungen und IT-Lösungen* und nach DIN ISO/IEC 9001 im Bereich des *Qualitätsmanagements*.



Gateway Security

Nutzen und Vorteile

Produkteigenschaften

- Konfiguration nach Ihren Anforderungen
- erweiterbar und flexibel
- Wartung und Hardwaretausch nächster Arbeitstag – NBD (Next Business Day)
- revisionsicher

Betrieb

- permanente Systemüberwachung / Monitoring (*Monitoring Base*)
- Überwachung und regelmäßige Auswertung der Log-Dateien
- Einspielen neuer Sicherheitspatches und Updates
- ständige Pflege

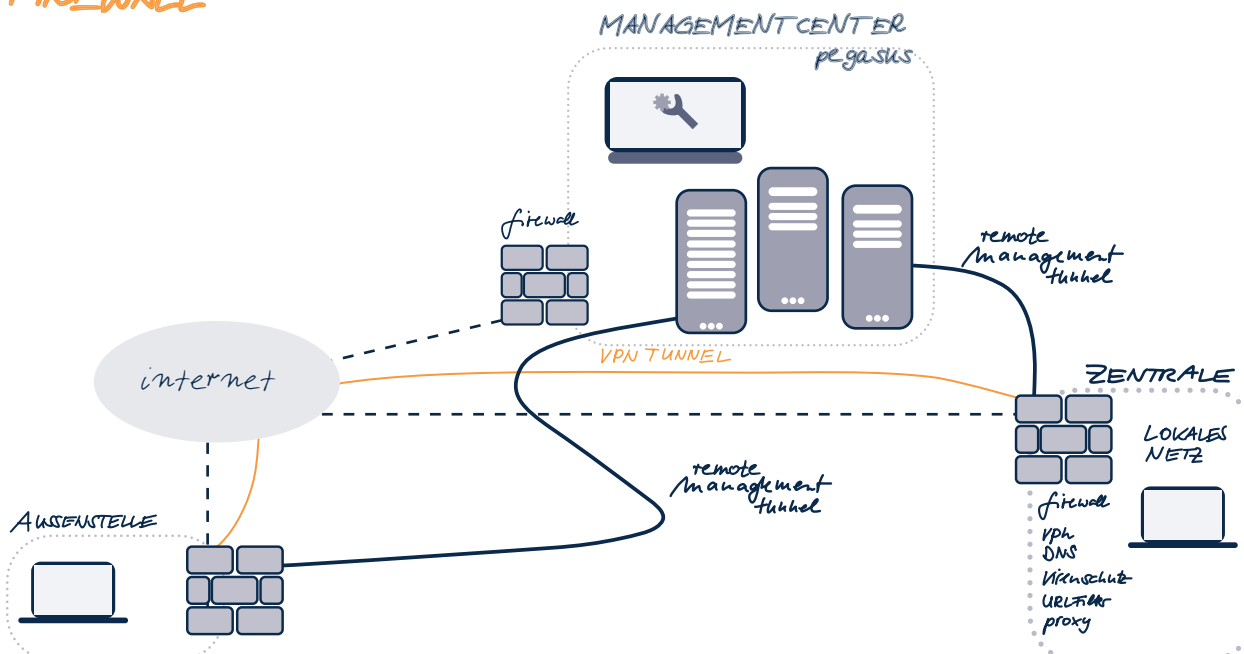
Support

- schnelle Reaktionszeit lt. vereinbarter SLA
- direkter Kontakt zum Hersteller mit dem Headquarter in Innsbruck
- Betrieb durch zertifizierte erfahrene Mitarbeiter

Gesetzliche Regelungen

- Beachtung gesetzlicher Vorschriften
- Haftungsverlagerung

FIREWALL



Gateway Security

Leistungsbeschreibung

Eine Leistungsbeschreibung wird individuell für Ihre Unternehmensbedürfnisse erstellt. Die zur Verfügung stehenden Features entnehmen Sie aus der untenstehenden Tabelle. Maßgeschneiderte SLA (Service Level Agreements) runden das Servicekonzept der *pegasus IT* für Ihren Geschäftserfolg ab!

Features

Firewall Typen (Auszug)		F 12	F 18 RevB	F 80 ReVB F82.DSLx	F 180 B	F 183 / F 183 R	F 280 RevC	F 380 RevB	F 400 RevC STD / F20	virtuell	
Network Security	Firewall [Gbps]	1,2	2,0	2,0/1,5	3,2	2,0/2,1	6,0	8,5	13	HW-abhängig	
	Intrusion Prevention [Mbps]	400	600	600/400	1 Gbps	580/790	2,0 Gbps	2,5 Gbps	4,2 Gbps		
	VPN Server ¹ [Mbps]	220	720	720/240	800	300	1,8 Gbps	2,1 Gbps	3,6 Gbps		
	Threat Protection ² [Mbps]	230	380	380	1,0 Gbps	600	1,5 Gbps	1,7 Gbps	3,1 Gbps		
User-Empfehlung	FW/VPN [max]	25	25	50	100	150	175	> 250	> 500	Lizenz-abhängig	
	+ Contentsec./ ATD [max]	10	10	25	65	85	125	> 200	> 400		
	+IPS/SSL Intercep/WAN Opt. [max]	5	5	10	40	60	100	> 150	> 250		
Hardware	Formfaktor	Desktop	Desktop	Desktop	Desktop	Desktop o. Hutschiene (R-Modell)	Desktop	19" 1 HE	19" 1 HE	HW-abhängig	
	1 GB Ethernet	5x	4x	4x	12x	6x 5 x (R)	12x	8x	8x		
	1 GB Fiber SFP	-	-	-	4x	2x	4x	-	- STD / 4x (F20)		
	10 GB Fiber SFP+							2x	2x		
	Integrated WiFi	-	-	✓	✓	✓	✓	-	-		-
	max. Storage [GB]	80	80	50	100	80	80	80	80		30
Routing	OSPF/RIP/BGP	✓	✓	✓	✓	✓	✓	✓	✓	✓	
VPN	IPSEC	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	TINA (erweiterte Funktionen)	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	Adv. Remote Access	-	optional	optional	optional	optional	optional	optional	optional	optional	
	Stateful Deep Inspection	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Security	Application Control	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	SSL Interception	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	WEB Filter	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	IPS / IDS	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	Malware Protection	-	optional	optional	optional	optional	optional	optional	optional	optional	
	Advanced Threat Protection	-	optional	optional	optional	optional	optional	optional	optional	optional	
SD-WAN & Konnektivität	MFA	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	App Based Provider Selection	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	Dynamic Bandwidth Detection	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	Traffic Shaping	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	Performance Based Transport Selection	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	Failover and Link Balancing	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	Azure Virtual WAN	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	Link Aggregation	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Logging & Statistics	Log Files (>1 Tag)	-	-	-	✓	✓	✓	✓	✓	✓	
	Statistic Files	-	-	-	✓	✓	✓	✓	✓	-	

Weitere Enterprise Modelle (> F400) auf Anfrage.

¹ Der angegebene Wert bezieht sich auf folgende technische Umsetzung der VPN-Tunnel-Konfiguration: Verschlüsselung AES128, Authentifizierung noHash, Transport UDP.

Bei BSI-konformer Einrichtung ergeben sich entsprechend geringere Werte (Faktor >2).

² Der angegebene Wert bezieht sich auf Werte mit allen aktivierten Securityfeatures (FW, VPN, IPS, AV, AppControl, ATP)

¹⁺² Die Durchsatzwerte beziehen sich auf das komplette Chassis mit allen verfügbaren Interfaces.

verfügbar als:

on premise IT ✓
managed IT ✓
cloud IT ✓