it-securitygroup

SECURE FIREWALL

The better way to protect your network

Secure Firewall bietet Sicherheit auf höchstem Niveau

Secure Firewall ist eine in Deutschland hergestellte hochsichere Application Level Firewall mit integriertem Web-Management, die eigens zur Absicherung von sensiblen Netzwerken konzipiert wurde. Sie schützt den Übergang verschiedener Netzsegmente (u. a. auch zu demilitarisierten Zonen), indem sie diese Netze physikalisch voneinander trennt.

Sie unterscheidet sich daher deutlich vom Konzept der „Stateful Inspection Firewall“ und bietet ein sehr viel höheres Sicherheitsniveau. Die Firewall verfügt über eine modulare Architektur und lässt sich sehr einfach in fast jede bestehende Netzwerkinfrastruktur integrieren.

Secure Firewall besteht aus einem gehärteten Betriebssystem, der eigentlichen Firewall-Software und dem integrierten Management. Sie vereint höchsten Sicherheitsstandard mit hoher Performance und einer sehr einfachen Bedienbarkeit.

Bedienerfreundliche Administration

Secure Firewall lässt sich von jedem Arbeitsplatz aus über einen Webbrowser administrieren. Der Zugang erfolgt dabei auf sichere Weise mittels SSL-Verschlüsselung (Client-Zertifikat) und durch Authentisierung des Administrators.

Alle Menüs innerhalb der Administration sind klar und übersichtlich strukturiert, sodass alle Sicherheitsfunktionen komfortabel verwaltet und überwacht werden können.

Die intelligente Architektur der Firewall schließt eine Fehlbedienung sogar faktisch aus.

Hohe Performance, Stabilität und Hochverfügbarkeit

Secure Firewall ermöglicht einen sehr hohen Datendurchsatz für alle Proxies auf Applikationsebene. Die Firewall-Software ist vor allem bei Behörden langjährig praxiserprobt und besticht durch ihre Stabilität und sehr hohe Zuverlässigkeit.

Über zwei redundante Gateways lässt sich Secure Firewall problemlos auch hochverfügbar einsetzen. Fällt ein System aus, übernimmt automatisch dann das zweite System dessen Funktionalität.

Welche Vorteile bietet Secure Firewall?

- Sicherer Rundumschutz durch eXtended Unified Threat Management (XTM)
- Extrem hoher Sicherheitsstandard
- Schnelle und einfache Inbetriebnahme sowie intuitive Administration
- Strukturierte Regelübersicht
- Detaillierte Zustandsmeldungen und Berichte
- Keine Lizenzbeschränkung im Hinblick auf die Anzahl der Benutzer oder Netzwerkverbindungen.

IT-Security Group
Sudetenstr. 2 b
61206 Wöllstadt
Deutschland

Tel: +49 6034 30 64 54
Fax: +49 6034 30 64 97
info@it-securitygroup.de
www.it-securitygroup.com

it-securitygroup

SECURE FIREWALL
The better way to protect your network

TECHNISCHE DATEN

HARDWAREANFORDERUNGEN

- Server mit folgender Minimalausstattung: VGA-Grafikkarte, 2 Netzwerkkarten, CDROM/DVD-Laufwerk, Festplatte > 8GB, serielle Schnittstelle, USB-Slot(s)
- Netzwerkkarten: Gigabit- und/oder Fast-Ethernet (bis zu 10 Netzwerkkarten)

SOFTWARE / BETRIEBSSYSTEM

- Speziell gesichertes und gehärtetes Linux OS, basierend auf Kernel 2.6

APPLICATION GATEWAY

- Single- oder Multi-homed

VIRTUAL PRIVATE NETWORK (VPN)

- OpenVPN-Zugang mit Benutzer-Zertifikaten und/oder Site-to-Site

PROXIES

- AntiVIRUS: HTTP(S), FTP, ESMTP, POP3
- AntiSPAM: ESMTP, POP3
- transparent oder nicht-transparent:
- HTTP(S), FTP, POP3, RTSP, TELNET, NNTP, PING
- nicht-transparent:
- HTTPS Decrypter, ESMTP, NET8, MGNTP, DNS

GENERISCHE RELAYS

- transparent oder nicht-transparent: TCPR, UDPR
- doppelt transparent: TCPR

AUTHENTISIERUNG

- Local Authentication System: Passwort, Einmal-Passwort (SKey), Mobile Authentication Service (MAS), IDENTD
- Remote Authentication System: LDAP, RADIUS

INTRUSION DETECTION

- Host Intrusion Detection System mittels AIDE

HOCHVERFÜGBARKEIT

- Jeweils zwei redundante Gateways im Aktiv – Aktiv (Loadsharing) oder Aktiv – Passiv (Hot Standby) Modus, basierend auf Heartbeat Version 2

PRIMÄRE SICHERHEITSMECHANISMEN

ZUGRIFFSKONTROLLE AUF NETZWERKEBENE

- Nur zugelassene Verbindungen können aufgebaut werden.

ZUGANGSKONTROLLE AUF BENUTZEREBENE

- Nur authentisierte Benutzer erhalten Zugriff auf einzelne Systeme oder Systemgruppen.

VERSCHLÜSSELTE ADMINISTRATION

- Der Management-Zugriff erfolgt vollständig verschlüsselt entweder über HTTPS (geschützt durch ein Client-Zertifikat) oder per SSH.

ADMINISTRATION VON ZUGRIFFSRECHTEN

- Ein Zugang ist nur dann möglich, wenn Protokolle und Dienste durch den Administrator definiert und zugelassen sind.

VOLLE KONTROLLE AUF APPLIKATIONSEBENE

- Benutzer können nur die notwendigen Kommandos der für ihre Arbeiten wichtigen Dienste (wie z.B. HTTP oder FTP) nutzen. Kommandos, die missbraucht werden könnten, stehen somit erst gar nicht zur Verfügung. Zudem lassen sich Dateninhalte (auch über HTTPS) an zentraler Stelle auf schädliche Inhalte (Malware, Viren) überprüfen.

ISOLATION VON DIENSTPROGRAMMEN

- Alle Dienste erfolgen stets über spezielle Proxy-Applikationen. Jeder Proxy arbeitet dabei mit eingeschränkten Rechten in einem isolierten Bereich des Betriebssystems.

BEWEISFÜHRUNG, LOG-ANALYSE UND ALARMFUNKTION

- Alle sicherheitsrelevanten Ereignisse können protokolliert und analysiert werden oder führen zusätzlich zu einer Alarmierung.

LIZENZIERUNG

Die Lizenzierung erfolgt mittels USB-Token.

IT-Security Group
Sudetenstr. 2 b
61206 Wöllstadt
Deutschland

Tel: +49 6034 30 64 54
Fax: +49 6034 30 64 97
info@it-securitygroup.de
www.it-securitygroup.com