

GateDefender Integra



GateDefender Integra SB



GateDefender Integra 300

Allgemeine Eigenschaften

Betriebsmodus (konfigurierbar)	Plug & Protect	Plug & Protect
Webbasierte Konsole mit Fernzugriff	✓	✓
Systemlastanzeige	✓	✓
Ansicht jeder Schutzaktivität	✓	✓
Anpassungsfähige Berichte und Warnungen	✓	✓
Graphische Aktivitätsberichte	✓	✓
Aktualisierung von Datenbanken und Signaturdateien	alle 90 Minuten	alle 90 Minuten
Anzahl der Netzknoten	50	250
Zentrale Überwachung	SNMP and Syslog	SNMP and Syslog
Zeitsynchronisation	NTP	NTP

Firewall

Firewall: Durchsatz	400Mbps	850 Mbps
Gleichzeitige Verbindungen	275.000	550.000
NAT-basierte Richtlinie	✓	✓

VPN

Dedizierte Tunnel	unbegrenzt	unbegrenzt
Verschlüsselungsverfahren	3DES, AES, Blowfish, Twofish, Serpent	3DES, AES, Blowfish, Twofish, Serpent
Unterstützung	Hub and spoke	Hub and spoke
Dienste	PPTP, L2TP, IPSec, SSL	PPTP, L2TP, IPSec, SSL
Validierung mit RADIUSservern	✓	✓

IPS/IDS

IPS-Angriffe	+ 4500	+ 4500
Automatische Echtzeitaktualisierungen	✓	✓

Malware-Schutz

Gescannte Protokolle	HTTP, FTP, SMTP, POP3, IMAP4 and NNTP.	HTTP, FTP, SMTP, POP3, IMAP4 and NNTP.
Viren, Würmer, Trojaner, Dialer und Jokes	✓	✓
Spayware und Phishing	✓	✓
Unbekannte Bedrohungen	✓	✓
Schwachstellen	✓	✓
Hackertools	✓	✓
HTTP-Durchsatz	31 Mbps	80 Mbps
SMTP-Leistung	20 Nachrichten /sek	160 Nachrichten /sek

Content-Filter

Filterung von Transportprotokollen	HTTP and FTP	HTTP and FTP
Filterung von E-Mail und News-Protokollen	SMTP, POP3, IMAP4 and NNTP	SMTP, POP3, IMAP4 and NNTP
Getrennte Aktionen für ankommenden & abgehenden Verkehr	✓	✓
Scannen verschachtelter Nachrichten und ihrer Anhänge	✓	✓

Dateifilterung

Mit mehreren oder abgeschnittenen Erweiterungen	✓	✓
Mit Makros oder Kennwörtern	✓	✓
Verdächtige komprimierte Dateien	✓	✓
ActiveX-Controls oder Java-Applets	✓	✓

Nachrichtenfilterung

Nach Textinhalt mit Mustersuche	✓	✓
Verschachtelt	✓	✓
Missgestaltet oder fragmentiert	✓	✓

Spamschutz

Gescannte Protokolle	SMTP, POP3 and IMAP4	SMTP, POP3 and IMAP4
Qualität des Scannens	mehr als 300.000 Algorithmen	mehr als 300.000 Algorithmen
Filtertypen	Bayes, heuristisch, lernfähig usw.	Bayes, heuristisch, lernfähig usw.
Konfigurierbarer Empfindlichkeitsgrad	ja (hoch, mittel oder niedrig)	ja (hoch, mittel oder niedrig)
Verschiedene Aktionen für 'Spam' und 'potenziellen Spam'	✓	✓
Verschiedene Quarantäne für 'Spam' und 'potenziellen Spam'	✓	✓
Anpassbare Whitelist und Blacklist	ja (IP, Domain und Adresse)	ja (IP, Domain und Adresse)

Web-Filterung

URL-Filterung nach Kategorie	mehr als 60 Kategorien	mehr als 60 Kategorien
Anpassbare Whitelist und Blacklist	✓	✓
Liste von der Filterung ausgenommener VIP-Anwender	✓	✓

Hardwarespezifikationen

Ports	4 x 10/100/1000	8 x 10/100/1000
Mikroprozessor	Intel Celeron M, 600 MHz	Intel Pentium IV 3.4GHz
RAM:	1024 MB	1 GB
Festplatte:	80 GB	80 GB
Abmessungen (mm)	272 x 195 x 44 mm	429 x 382 x 44
Masse	2 kg	11.1 kg / 24.47 lbs
Formfaktor	1U Desktop	1U 19" Rackmount
Zertifizierungen	CE / FCC / UL	CE / FCC
Betriebstemperatur	5°C - 40°C	5°C - 35°C
Lagertemperatur	0°C - 75°C	-20°C - 70°C
Feuchtigkeit	20% - 90% nicht kondensierend	20% - 90% nicht kondensierend

Weitere Daten

Kundendienst ständig rund um die Uhr	✓	✓
--------------------------------------	---	---

Zentraler Umgebungsschutz gegen alle Internet-Gefahren

Firewall • VPN • IPS • Malware-Schutz • Content-Filter • Spamschutz • Web-Filter



Panda GateDefenderIntegra

Plug&Protect

PANDA | 20th Anniversary
SECURITY 1990-2010

Plug and Protect

Das einzige "Plug-and-Protect"-UTM: **Panda GateDefender Integra** ist das einzige UTM-Gerät auf dem Markt, das sofort nach Anschluss zu schützen beginnt. Um Anwender von Beginn an zu schützen, sind Malware-Schutz, Spamschutz und Web-Filterung standardmäßig aktiviert. Die anderen Schutzmodule müssen aus technischen Gründen mit Hilfe des Kundendienstes von Panda konfiguriert werden.

Präventiver Netzwerkschutz in einem einzigen Gerät

Ungefähr 99 % der Bedrohungen von Unternehmensnetzen werden über das Internet übertragen. Dies macht die Gateway-Verbindung zu einem kritischen Punkt für die Sicherheit im Netz. Wird an dieser Stelle ein Schutz eingesetzt, verringert sich die Belastung von Servern und Workstations durch Scannen und Desinfizieren ganz wesentlich. Dadurch können Probleme schon abgewendet werden, bevor sie das interne Netz überhaupt erreichen.

Wegen der Verschiedenartigkeit der möglichen Bedrohungen müssen verschiedene Technologien unter einer einzigen, leicht zu bedienenden Schnittstelle integriert werden. Diese sollte gleichzeitig die Sicherheit an einem kritischen Punkt des Netzes wie etwa bei der Internetverbindung zentralisieren kann, um die internen Netze ausreichend zu schützen.

Panda GateDefender Integra ist ein vereinheitlichtes Umgebungsschutzgerät, das über eine einzige einfache Schnittstelle für den gesamten Schutz im Unternehmensnetz präventiv vor Bedrohungen aller Art, sei es auf der Ebene des Netzes oder auch vor unerwünschtem Inhalt, schützt.

Außerdem können Administratoren damit die Aktivität jedes Schutzmoduls graphisch und intuitiv überwachen, um die Sicherheit im Netz zu verbessern.

Firewall
Intrusion Prevention System (IPS)
VPN

Malware-Schutz¹
Content-Filter
Spamschutz
Web-Filterung



¹ Enthält Schutz vor Viren, Würmern, Trojanern, Spyware, Dialern, Jokes, Phishing, Hackertools, Sicherheitsrisiken und Bedrohungen, die noch nicht in der Signaturdatei katalogisiert worden sind.

Zwei Modelle - je nach Ihren Anforderungen

Panda GateDefender Integra SB



Panda GateDefender Integra 300



ALLGEMEINE VORTEILE:

- **Plug and Protect**
Keine Konfiguration notwendig. Einfach anschließen und sofort geschützt sein.
- **Vollständiger Schutz**
Umfassender Schutz gegen alle Netzwerk und Content basierten Gefahren in einem einzigen Gerät.
- **Optimierte Ressourcenauslastung**
Verhindert unerwünschten Netzwerk-Traffic und ungewollte Verbindungen.
- **Gesteigerte Produktivität**
Befreit das Netzwerk von Spam-Mails und verhindert den Zugriff auf unangebrachten Inhalt aus dem Internet.
- **Vollständige Kontrolle**
Echtzeitzugriff auf Informationen über die Aktivität des Schutzsystems.
- **Automatische Sicherheit**
Nachdem der Schutz konfiguriert ist, aktualisiert er sich automatisch und erfordert nur ein Minimum an Wartung.

Schutz vor Bedrohungen aus dem Internet

Firewall

Maximale Kontrolle

Die Kommunikation zwischen allen Bereichen, Anwendern, Gruppen usw. des Netzes wird über das Firewall-System kontrolliert und durch den Administrator überwacht. Dadurch wird die höchstmögliche Leistung im Internet sichergestellt.

Es gibt zwei Arten der Filterung:

1. Statisch auf der Netzwerkebene.
2. Dynamisch auf Anwendungsebene.

1. Die statische Filterung auf der Netzwerkebene beruht auf Regeln, die durch den Administrator für den ankommenden und abgehenden Verkehr definiert werden.

2. Die dynamische Filterung auf der Anwendungsebene mit 'Stateful Inspection' überwacht den Status und den Inhalt der Basic Communication in allen Protokollen und der Advanced Communication in FTP, PPTP, L2TP, IPSEC, den Status der Verbindung, Zeitüberschreitungen, aufgebaute Verbindungen usw. Außerdem umfasst sie eine 'Tiefenuntersuchung von Paketen', das Scannen des Inhalts von Paketen zur Untersuchung von Nachrichten in HTTP, FTP, SMTP, IMAP, POP3 usw., wenn weitere Module freigegeben sind.

VPN-Dienst

Sichere Übertragungen

Der VPN-Dienst stellt sichere Kommunikationswege mit fernem Anwendern oder anderen Büros bereit, die sich perfekt an die aktuelle Arbeitsumgebung des Unternehmens anpassen.

Er ermöglicht, dass sich ferne Computer über das Internet mit dem internen Netz verbinden, wobei die übertragenen Daten bei der Quelle verschlüsselt und am Ziel entschlüsselt werden, sodass sie nicht in falsche Hände gelangen können. Dieser Dienst kann in einer Host-zu-Host-, Host-zu-Netz- und Netz-zu-Netz-Konfigurationen arbeiten. Er unterstützt folgende Protokolle im Server-Modus: IPSec, SSL, L2TP und PPTP. Außerdem arbeitet er unter SSL und IPSec im Client-Modus.

Intrusion Prevention System (IPS)

Verstärkte Sicherheit

Das System verhindert die schnelle Ausbreitung äußerer Angriffe, die die herkömmliche Virenabwehr unterlaufen.

Es stellt eine signaturbasierte Erkennung von Eindringversuchen bereit, die eine Schädlingssignaturdatei nutzt, welche von Panda Security geliefert und alle 90 Minuten aktualisiert wird. Das System scannt IP, ICMP, TCP und UDP. Administratoren können es so konfigurieren, dass es die erkannten Eindringversuche automatisch blockiert, und können für jede Regel eine Schwelle angeben, sodass Fehlmeldungen verringert werden.

Schutz vor unerwünschtem Inhalt

Malware-Schutz

Komplettschutz

Dieser ständig aktualisierte Schutz blockiert alle Arten von Malware einschließlich solcher, die noch nicht im Katalog zu finden sind.

Er bietet sowohl proaktiven als auch reaktiven Schutz vor allen Bedrohungen, die über die sechs am häufigsten verwendeten Internet-Protokolle (HTTP, FTP, SMTP, POP3, IMAP4 und NNTP) übertragen werden. Diese Bedrohungen umfassen: Viren, Spyware, Trojaner, Würmer, Dialer, Jokes, Phishing und andere Bedrohungen wie etwa Hackertools oder Sicherheitsrisiken. Dank seiner heuristischen Scanfähigkeiten blockiert es auch unbekannte Viren.

Content-Filter

Anpassbarkeit

Der Schutz kann durch Netzadministratoren vollständig angepasst werden, um ihn auf die Unternehmenssicherheitsrichtlinie auszurichten.

Er filtert potentiell gefährlichen Inhalt in komprimierten Dateien, ausführbaren Dateien, ActiveX Controls usw. Er bietet eine separate Konfiguration für E-Mail/Newsgruppen-Protokolle und File Transfer-/Internet-Protokolle. Der Administrator kann sowohl die Dateien und Inhaltstypen als auch den zu filternden Textinhalt konfigurieren.

Spamschutz

Saubere E-Mails

Dadurch, dass das Spamschutzsystem Junk-Mail-Verkehr verhindert, optimiert es die Netzwerkressourcen und befreit die Anwender vor unnötigen und zeitraubenden Nachrichten.

Alle ankommenden Nachrichten werden unter Verwendung von Multifunktionsanalysetechniken (Bayes-Regel, heuristisch, Regeln ...) geprüft und entweder als 'Spam', als 'potenzieller Spam' oder als 'kein Spam' klassifiziert. Junk-Mail wird blockiert, bevor sie die Posteingänge der Anwender erreicht, oder der Betreff dieser Nachrichten wird gekennzeichnet, damit die Anwender im Netz keine Zeit für sie verschwenden.

Web-Filter

Erhöhung der Produktivität

Der Web-Filter optimiert die Produktivität der Mitarbeiter, indem er den Zugriff auf Internet-Inhalt, der nichts mit der Arbeit zu tun hat, blockiert.

Er ermöglicht, dass Netzwerkadministratoren Kategorien von unproduktivem Inhalt definieren und autorisierte sowie nicht autorisierte Webseiten auflisten. Dadurch können Administratoren die Verwendung der Unternehmensnetzressourcen kontrollieren und den Zugriff auf anstößige, gewalttätige oder aus anderen Gründen unangebrachte Web-Inhalte verhindern.