

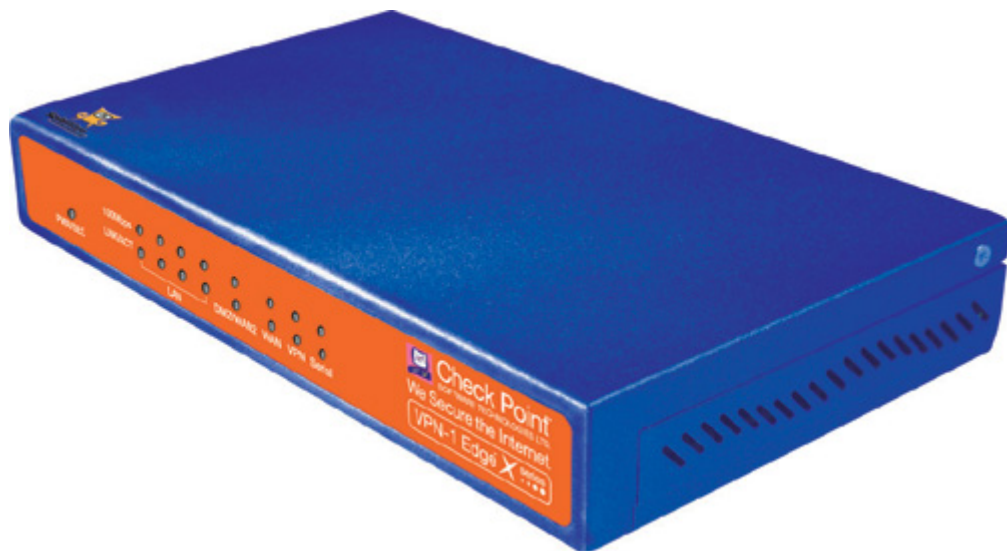


Für die Firewall Appliance

CHECK POINT VPN-1 EDGE XU

Die VPN-1 Edge Baureihen bieten Unternehmen aller Größen eine erstklassige Sicherheit mit einer Vielzahl an hervorragenden Services zu einem günstigen Preis.

Aufgrund der erstklassigen Testergebnisse und den vielseitigen Einsatzmöglichkeiten erhält die VPN-1 Edge XU den **ProtectStar-AWARD** für das Jahr 2004.



Einleitung

Die Firewall-Appliance "**VPN-1 Edge XU**" von **Check Point Software Technologies** zum Schutz und zur sicheren Anbindung von Filialen und Außenstellen an Unternehmensnetze ist mit der bewährten Stateful Inspection- und Application Intelligence-Technologie ausgestattet und bietet daher Schutz sowohl auf Netzwerk- als auch Applikationsebene.

Zum Verständnis:

VPN-1 Edge Appliances gibt es in den beiden Baureihen S und X. Die X-Serie verfügt über zusätzliche Funktionen wie Gateway High Availability, Backup ISP, Dial Backup VLAN-Unterstützung und Static NAT sowie höhere Firewall- und VPN-Durchsatzraten und Site-to-Site-VPN.

Das in unseren Testreihen verwendete Modell „**XU**“ ist das Flaggschiff der VPN-1 Edge Baureihe und hat keine Beschränkungen auf die Anzahl der an dem Gerät angeschlossenen Benutzer (das „U“ steht für „unlimited users“). Neben diesem Modell gibt es beispielsweise noch „**X16**“ und „**X32**“. Hierbei stehen die Zahlen für die maximale Anzahl an Benutzern, die an dem Gerät angeschlossen werden können.

Sicherheit

Die meisten Firewalls, die heutzutage in den unterschiedlichen Unternehmen eingesetzt werden, verhindern Angriffe auf der Netzwerkebene. Aus diesem Grund nutzen Hacker vermehrt Schwachstellen auf der Applikationsebene, um beispielsweise Viren und Trojaner in Unternehmensnetzwerke einzuschleusen. Auch moderne Kommunikationstechnologien wie Voice over IP bieten unerwünschten Eindringlingen viele weitere Angriffspunkte. Die Check Point-Lösungen sind die einzigen, die sowohl auf der **Netzwerk-** (Layer 3) als auch auf der **Applikationsebene** (Layer 7) effektiven Schutz bieten können.

In unseren Testreihen haben wir die **VPN-1 Edge XU** Appliance mit der Software-Version **4.5** detailliert und die Lupe genommen und können dem Security Allrounder eine ausgezeichnete Schutzwirkung bestätigen, die einen umfassenden und sicheren Schutz für Unternehmen bietet.

Die VPN-1 Edge XU hat an den Tagen unseres Testverfahrens alle zum Zeitpunkt bekannten **2152** verschiedenen **Angriffs- und Sicherheitstest** erfolgreich abgewehrt. Wir konnten in den verschiedenen Standardeinstellungen der Appliance auch keine offenen Ports finden, die für einen externen Angreifer nutzbar sein könnten.

Die Denial-of-Service Schutzfunktionen, die so genannte „DoS-Protection“ und die Anti-spoofing Sicherheitsvorkehrungen funktionierten in unserem Test ebenfalls einwandfrei.

Unseren achtstündigen Dauer-Penetrationstest hat die Appliance ebenfalls erfolgreich absolviert.

Eine weitere Schutzfunktion bietet die passwortgeschützte Web-Konsole, die nur autorisierten Personen Zugang verschafft. Der Zugang zur Konsole kann über den Port 80 (HTTP), sowie über den verschlüsselten Port 443 (HTTPS) aufgerufen werden.

So ist bei der VPN-1 Edge XU auch das Passwort der Konfigurationskonsole vor einer möglichen Ausspähung durch Netzwerksniffer gesichert.

Die Schutzfunktionen der Stateful Packet Inspection Firewall lassen sich durch einen „Schieberegel“ in drei verschiedene Stufen **LOW**, **MED** und **HIGH**, einstellen.

Auch wenn solche „Schieberegler“ bei Firewalls unter Experten i.d.R. nicht beliebt sind, so müssen wir speziell bei den **VPN-1 Edge** Baureihen eine Ausnahme machen, denn die unterschiedlichen Sicherheitslevels sind perfekt an die Bedürfnisse von Unternehmen angepasst worden. In allen drei Stufen werden alle eingehenden Verbindungen strikt kontrolliert und gegebenenfalls blockiert.

Mit dem Gerät können (theoretisch) bis zu **unendlich** viele IPSec VPN Tunnel betrieben werden. Hier können Unternehmen sowohl mit DES/3DES, als auch mit AES verschlüsseln.

Die automatische Update-Funktion sorgt für einen lückenlosen Schutz gegen neue Bedrohungen und sich schnell verbreitende Attacken. Pünktlich alle zwei Stunden sucht die VPN-1 Edge XU Appliance automatisch nach möglichen verfügbaren Firmware-Updates.

Benutzerfreundlichkeit

Bei der Benutzerfreundlichkeit haben wir eine Sache zu bemängeln: Es existieren derzeit noch keine Informationen, Handbücher, Datenblätter, usw. in deutscher Sprache, sondern sind nur in Englisch verfügbar.

Die Installation der **VPN Edge XU** ist sehr anwenderfreundlich und der Installationsassistent hilft dem Anwender das Gerät in wenigen Schritten zu konfigurieren.

Leider ist auch das Web-Interface in englischer Sprache. Jedoch ist das Interface optisch ansprechend und sehr übersichtlich gehalten, so dass alle Funktionen und Einstellungen leicht vorgenommen werden können.

Bei der Installation und Konfiguration des Gerätes dürfte es keine Schwierigkeiten oder Probleme geben. Unerfahrenen Anwendern helfen das mitgelieferte knapp zweihundertfünzigseitige Handbuch, sowie die Schnellanleitung, die alle relevanten Schritte und Fragen sehr detailliert und anschaulich beantworten.

Außerdem steht dem Benutzer jederzeit auf der linken Seite des Konfigurationsmenüs durch anklicken des „Help“-Button eine praktische Online-Hilfe zur Verfügung.

Das manuelle Hinzufügen von Firewall-Regeln geschieht zum Beispiel mit Hilfe eines Wizards. Dieser Wizard ähnelt stark den, der softwarebasierten Personal Firewalls. Alle Eingaben können bequem per Mausclick vorgenommen werden.

Als Erstes kann der Anwender bei der Regeleinstellung der Firewall auswählen, ob er ein- oder ausgehende Verbindung erlauben oder blockieren möchte oder ob er eine spezifische Verbindung erlaubt und weitergeleitet werden soll.

Im zweiten Schritt wählt der Anwender, ob ein bestimmter Dienst, alle Dienste, ein spezifisches Protokoll (TCP, UDP, GRE, ESP), alle Protokolle oder einen Portbereich, erlaubt oder blockiert werden soll. Als letztes muss nur noch Quelle und Ziel festgelegt werden, in welche die gewünschte Verbindung erlaubt/blockiert werden soll. Fertig!

Auf der Rückseite der VPN-1 Edge Appliances ist zusätzlich ein **DMZ** (De-Militarized-Zone) Port angebracht, der es Unternehmen erlaubt, einen öffentlichen Server, wie Web-, Mail- und FTP-Server, ohne zusätzlichen Switch anzuschließen und gleichzeitig durch die Stateful Packet Inspection Firewall zu schützen.

Die zusätzlichen Funktionen wie zum Beispiel Gateway High Availability, Backup ISP, Dial Backup VLAN-Unterstützung und Static NAT und Site-to-Site-VPN sind für Unternehmen nützliche Werkzeuge, die in der VPN-1 Edge XU standardmäßig integriert sind.

Besonders gut hat uns unter dem Menüpunkt „**Reports**“ -> „**Active Computers**“ die grafische Darstellung gefallen, die dem Anwender Aufschluss darüber gibt, welche Computersysteme (Computername & MAC-Adresse) an der VPN-1 Edge XU angeschlossen sind. Zudem erfährt man unter diesem Menüpunkt auch, welche IP-Adresse die entsprechende Workstation oder Server hat und ob die IP-Adresse statisch ist oder beispielsweise via DHCP an das jeweilige Computersystem vergeben wurde.

Die Log-Datei lassen etwas zu wünschen übrig, denn aus ihnen kann der Anwender lediglich erfahren, dass ein Angriff stattgefunden hat. Diese Einträge werden in roter Farbe dargestellt. Was für ein Angriff genau getätigt wurde, bleibt fraglich. Dem Anwender ist nur ersichtlich, wann der Angriff (über das Protokoll TCP oder UDP) getätigt wurde und welcher Computer/Server auf welchem Port angegriffen wurde.

Durch einen Mausklick auf die IP-Adresse des Angreifers öffnet sich ein WHOIS-Fenster, in dem der Anwender mehr Informationen über den Angreifer bzw. dessen Provider erhalten kann.

Performance

Das Gerät arbeitete bei allen unseren Testreihen äußerst schnell und zuverlässig und wir konnten keine Leistungseinbußen oder Mängel bei der Performance in irgendeiner Art feststellen.

Die Stateful Inspection Firewall kann Durchsatzraten von **150** Mbps verarbeiten. Die VPN-Funktionen arbeiten im verschlüsselten Modus (3DES/AES) mit einer Durchsatzrate von **30** Mbps.

Zudem unterstützt die VPN-1 Edge XU Appliance bis zu **8.000** gleichzeitige Verbindungen.

Selbst bei unserem achtstündigen Dauer-Penetrationstest konnte weiterhin problemlos unter kleinen Einschränkungen mit der Appliance gearbeitet werden.

Support

Mit dem Erwerb des Gerätes erhält der Anwender ein Jahr lang Garantie und Softwareupdates inklusive.

Unter <http://www.checkpoint.com/techsupport> hat der Anwender von Produkten aus dem Hause Check Point, Zugriff auf eine umfangreiche Wissensdatenbank (Knowledgebase) und die am häufigsten gestellten Fragen (FAQ).

Interessenten können die Appliances nicht direkt bei Check Point, sondern bei einem autorisierten Reseller erwerben. Dieser ist dann für den Support und die gesetzlichen Gewährleistungen zuständig und erneuert auf Wunsch hin auch den jährlichen Supportvertrag.

Preis / Leistung

Mit einem Preis von **1.999 Euro** (netto) ist die **VPN-1 Edge XU** Appliance aufgrund ihrer nahezu perfekten Schutzwirkung, der Vielzahl an Funktionen und flexiblen Einsatzmöglichkeiten, zu anderen Firewall-Lösungen auf dem IT-Sicherheitsmarkt preiswert.

Das kleinste Gerät der VPN-1 Edge Baureihe, die **VPN-1 Edge S8**, ist übrigens schon ab einem Preis von **399 Euro** (netto) verfügbar und für bis zu acht Benutzer geeignet.

Fazit

Gerade für Firmen, die neben hohem Internet-Verkehr einen sicheren und anwenderfreundlichen Datentransfer zwischen externen Niederlassungen und Außendienstmitarbeitern und der Firmenzentrale per VPN bewältigen müssen, liefern die VPN-1 Edge Baureihen eine ausgezeichnete Lösung.

Besonders erwähnenswert sind die einfache Installation und Bedienung, die schnell einzurichtenden Sicherheitsregeln und der effektive Schutz sowohl auf der Netzwerk- (Layer 3) als auch auf der Applikationsebene (Layer 7).

Das zentrale Management, die Unterstützung von SmartCenter Pro und Provider-1 machen es einfach, aufwändige VPNs mit der One-Click-Technologie von Check Point in Minutenschnelle einzurichten.

Die Hochverfügbarkeit, Multi-ISP-Unterstützung, Backup ISP, Dial Backup, VLAN-Unterstützung, QoS, NAT-T, Static NAT und Dynamic Routing garantieren zu dem eine nahtlose Sicherheit und eine gute Investition in die Zukunft.

Die VPN-1 Edge XU Appliance von Check Point erhält aufgrund der erstklassigen Testergebnisse und den vielseitigen Einsatzmöglichkeiten den **ProtectStar-AWARD** für das Jahr 2004.