

Der Malware „Zoowärter“

*[Fragen und Antworten rund um
Sonicwall Firewalls und dem vitosecure
Vertrag der Vitodata AG]*



(Bildquelle: Fraunhofer Institut für Rechnerarchitektur und Softwaretechnik)



Inhaltsverzeichnis

Warum vertreibt die Vitodata AG nur Sonicwalls und keine weiteren Firewalls?	3
Kann kein anderer Anbieter die Firewall updaten (Firmware)?	3
Kann kein anderer Anbieter die Firewall updaten (Konfiguration)?	4
Warum reicht eine Softwarefirewall nicht für unseren Bedarf?	4
Warum setzen Sie nicht eine Softwarefirewall ein? Diese haben doch in Tests sehr gut abgeschnitten.	5
Warum kann keine Überwachung bei Nicht-Sonicwall Firewalls angeboten werden?	5
Wie hoch ist das Risiko, wenn ich „nur“ eine Hardwarefirewall einsetze ohne vitosecure Vertrag (UTM Dienste)?	6
Für den Preis des vitosecure Vertrages könnte ich mir jährlich eine neue Firewall mit den neusten Definitionen kaufen und installieren lassen. Warum?	7
Ich habe ein Kombigerät (Router/Firewall), genügt diese Sicherheit nicht? Der Hardwarelieferant meint, diese Sicherheit genüge, da es ja eine Hardwarefirewall ist.	8
Was ist der genaue Leistungsumfang vom vitosecure? Was machen all diese Dienste genau?	8
Weshalb kann der Global VPN Client nur auf einer Sonicwall und nicht auf einer anderen Firewall eingerichtet werden?	9
Weshalb kann allgemein eine VPN Verbindung jeweils nur zwischen zwei Geräte desselben Herstellers eingerichtet werden?..	9
Warum benötige ich eine fixe IP Adresse, wenn ich von zu Hause auf meine Praxis zugreifen möchte?	10



Warum vertreibt die Vitodata AG nur Sonicwalls und keine weiteren Firewalls?

Die Vitodata AG hat sich vor einigen Jahren für Sonicwall entschieden, weil diese Firma bezüglich Preis-/Leistung im Vergleich zu der Konkurrenz eine der besten Lösungen anbietet. Weitere Gründe sind ein anhaltender und erstklassiger Service, sowie eine hervorragende Managementsoftware, welche es der Vitodata AG erlaubt sämtliche vitosecure Firewalls zentral zu verwalten.

Unsere inzwischen sehr grosse Erfahrung mit Sonicwall Produkten garantiert dem Kunden einen erstklassigen Service und ein breites Know-how. Einen ähnlichen Service kann die Vitodata AG bei keinem anderen Hersteller bieten.

Diese Gründe sprechen für den Einsatz einer Sonicwall bei unseren Kunden, insbesondere dann wenn der Kunde einen vitosecure abschliessen will, da es diesen Vertrag NUR mit einer Sonicwall geben kann (dies ist eine technische Einschränkung). Weiter muss die Vitodata AG eine möglichst homogene Produktlandschaft anbieten können, wollen wir unsere Kunden optimal und effizient beraten.

Zusammenfassung: Sonicwall bietet eines der besten Preis-/Leistungsverhältnisse auf dem Firewall Markt und die Vitodata AG das dazu passende Know-how!

Kann kein anderer Anbieter die Firewall updaten (Firmware)?

Hat der Kunde einen vitosecure Vertrag mit der Vitodata AG abgeschlossen, dann kann dies von keinem anderen Anbieter vorgenommen werden und ist auch nicht nötig, da diese Dienstleistung ein Teil des vitosecure Vertrages darstellt.

Hat der Kunde keinen vitosecure Vertrag, dann steht ihm frei, wer die Updates der Firmware auf der Firewall tätigt. An dieser Stelle sei noch erwähnt, dass ein kostenloses Update der Firmware nur dann möglich ist, wenn die Sonicwall unter mysonicwall.com registriert wurde. Ab diesem Zeitpunkt ist ein Update jedoch nur während exakt 90 Tagen möglich.

Zusammenfassung: bei einem vitosecure: nein! Bei keinem vitosecure: kann jeder andere Anbieter einen Update durchführen.



Kann kein anderer Anbieter die Firewall updaten (Konfiguration)?

Hat der Kunde einen vitosecure Vertrag mit der Vitodata AG abgeschlossen, dann kann dies von keinem anderen Anbieter vorgenommen werden. Mit dieser Haltung will die Vitodata AG verhindern, dass Änderungen an der Sonicwall vorgenommen werden, welche zum einen für den Kunden schädlich sein könnten und zum anderen um sicherzugehen, dass zu einem späteren Zeitpunkt nicht die Vitodata AG wegen einer Fehlkonfiguration belangt werden kann. Hier gilt ganz klar folgendes Motto: „Zu viele Köche verderben den Brei“.

Hat der Kunde keinen vitosecure Vertrag, dann steht ihm frei, wer die Änderungen der Konfiguration vornimmt. In einem solchen Fall wird das Standardpasswort der Vitodata AG zurückgesetzt und dem Kunden das neue Passwort kommuniziert. Weiter wird kommuniziert, dass die Vitodata AG keine Haftung für die Konfiguration der Sonicwall übernehmen kann.

Zusammenfassung: bei einem vitosecure: nein! Bei keinem vitosecure: kann jeder andere Anbieter einen Update durchführen.

Warum reicht eine Softwarefirewall nicht für unseren Bedarf?

Grundsätzlich ist dies immer eine Frage der Sicherheit und des Know-hows des Kunden. Folgendes muss man wissen:

Vor- und Nachteile einer Hardwarefirewall (im Vergleich zu einer Softwarefirewall):

- + Blockt Verbindungen bevor diese ins Netzwerk oder auf dem Computer landen
- + Viel leistungsfähiger
- + Einfacher in der Handhabung (einmalig konfiguriert)
- + Möglichkeit für die Erstellung von VPN's
- + Möglichkeit auf Ebene des Netzwerks diverse Regeln und Sicherheitsmassnahmen zu konfigurieren
- Relativ hoher Anschaffungspreis (jedoch nur auf den ersten Blick)



Vor- und Nachteile einer Softwarefirewall (im Vergleich zu einer Hardwarefirewall):

- + Relativ geringer Anschaffungspreis, falls in einem Bundle mit einem Antivirus
- + Ist höchstens dann sinnvoll, wenn nur ein Computer sich im Netzwerk befindet
- Eine Verbindung wird erst auf dem Computer untersucht
- Das Netzwerk und allfällige andere Computer im Netzwerk sind ungeschützt
- Es kann nur die Verbindungen auf den Computer überwacht werden und nicht sämtliche Verbindungen im Netzwerk
- Bescheidene Möglichkeiten in der Konfiguration
- Keine Möglichkeit für die Erstellung von VPN's
- Aufwendige Konfiguration, ansonsten erscheinen dauernd irgendwelche Meldungen welche von 95% der Kunden nicht verstanden werden können

Zusammenfassung: aus den obengenannten sicherheitstechnischen Gründen und im Interesse der Informationssicherheit der Kunden kann die Vitodata AG den Einsatz einer Softwarefirewall nicht empfehlen.

Warum setzen Sie nicht eine Softwarefirewall ein? Diese haben doch in Tests sehr gut abgeschnitten.

Grundsätzlich ist diese Frage bereits in der obenstehenden Antwort zur Frage, warum eine Softwarefirewall nicht für den Bedarf eines Arztes genügt, enthalten.

Ein weiterer Grund ist hier auch der Preis. Zum Beispiel kostet die Jetico Personal Firewall pro Computer und Jahr ca. sFr. 60.- (Stand 03.2009). Wenn man dies in einer kleinen Praxis mit 3 Computern auf 3 Jahre hochrechnet, dann kostet diese Personal Firewall ca. sFr. 540.-! So gesehen, ist dies keine wirklich gute Investition, da für weniger Geld eine Hardwarefirewall gekauft werden kann, welche nicht nur bedeutend mehr Möglichkeiten bietet, sondern den Schutz standardmässig auch mind. 10 Computern im Netzwerk ermöglicht.

Zusammenfassung: Softwarefirewalls haben unter dem Strich das bedeutend schlechtere Preis-/Leistungsverhältnis als eine Sonicwall.

Warum kann keine Überwachung bei Nicht-Sonicwall Firewalls angeboten werden?

Weil eine solche Verwaltungssoftware oder Überwachungssoftware immer Hersteller spezifisch ist. Das heisst, dass die Verwaltungssoftware welche für Sonicwalls von der Vitodata AG eingesetzt wird, nur Sonicwalls überwachen kann. Es handelt sich hier um eine rein technische Limitation und nicht um eine politische.

Uns ist bis heute (Stand 03.2009) keine Verwaltungssoftware bekannt, welche Firewalls Hersteller unabhängig verwalten resp. überwachen kann und wahrscheinlich wird dies auch in Zukunft nicht möglich sein, da dies technisch nicht ganz einfach lösbar ist.

Zusammenfassung: dies ist eine rein technische Begrenzung und keine politische!



Wie hoch ist das Risiko, wenn ich „nur“ eine Hardwarefirewall einsetze ohne vitosecure Vertrag (UTM Dienste)?

Hier würde bereits ein Blick auf die untenstehende Tabelle reichen, in welche stichwortartig die Unterschiede aufgezeigt sind.

Im Detail können folgende Zahlen belegen, dass in den letzten Jahren die Anzahl an sogenannter Malware exorbitante Dimensionen angenommen haben (Quelle: Frauenhofer Institut für Rechnerarchitektur und Softwaretechnik):

- **Allgemeine Zahlen zu Viren und Trojanern etc:**
 - + Anzahl von Viren und Trojanern in 1997: 17'000
 - + Anzahl von Viren und Trojanern in 2006: 222'000
 - + Steigerung der Anzahl von Viren und Trojanern in den Jahren 1997 bis 2006 in Prozent: 1'306
 - + Anteil der klassischen Viren an der Gesamtzahl der Schadprogramme in 2000 in Prozent: 81
 - + Anteil der klassischen Viren an der Gesamtzahl der Schadprogramme in 2007 in Prozent: 1
 - + Neue Malware-Varianten, die in 2007 entdeckt wurden: 5'500'000
 - + Anzahl von neuen Schädlingen, die Experten von AV-Test in den ersten sieben Tagen des Jahres 2008 entdeckt haben: 117'480
 - + Zahl der bekannten Viren für Windows-Systeme in 2007: 60.000

- **Schwachstellen und Sicherheitsrisiken:**
 - + Zahl der seitenspezifischen Schwachstellen, die im zweiten Halbjahr 2007 registriert wurden: 11'253
 - + Zahl der „Baukästen“ für Phishing-Software, auf die 26 Prozent aller weltweiten Phishing-Seiten in 2007 zurückgehen: 3
 - + Preis, den unveröffentlichte Sicherheitslücken auf dem Schwarzmarkt erzielen, in Euro: 35'000



- **Kriminalität:**
 - + Anteil der gestohlenen Online-Identitäten in Deutschland, die auf das Konto von Malware gehen, in Prozent: 90
 - + Zahl der beim Bundeskriminalamt (BKA) gemeldeten Phishing-Fälle in den ersten zehn Monaten in 2007: 3'100
 - + Durchschnittliche Schadenssumme dieser Phishing-Fälle gerundet in Euro: 4'500
 - + Gesamte Schadenssumme dieser Phishing-Fälle gerundet in Euro: 14'000'000
 - + Anteil der Kreditkarten-Informationen an gehandelten Warengruppen auf Untergrund-Servern in der ersten Hälfte von 2007 in Prozent: 22
 - + Startkapital des ersten Kopfgeld-Fonds, den Microsoft 2003 u.a. für Hinweise zur Ergreifung und Verurteilung von Viren- und Würmer-Programmierern ausgestattet hat, in Dollar: 5'000'000
 - + Preis, den Spezialtrojaner auf dem Schwarzmarkt erzielen, in Euro: >10.000

Zusammenfassung: anhand dieser Zahlen braucht man kein Sicherheitsexperte zu sein, um festzustellen, dass im Bereich Malware ein enormes Potential steckt. Die Internetkriminellen beschreiten immer raffiniertere Wege, um erfolgreich zu sein! Damit man sich erfolgreich dagegen schützen kann, muss man auf dem aktuellen Stand der Dinge sein und dies wird im Moment ganz klar durch die sogenannten UTM Dienste bewerkstelligt (siehe die Erklärungen weiter unten)!

Für den Preis des vitosecure Vertrages könnte ich mir jährlich eine neue Firewall mit den neusten Definitionen kaufen und installieren lassen. Warum?

Natürlich kann man dies aus dieser Perspektive betrachten... nur, dies entspricht NICHT denselben Leistungen die im vitosecure enthalten sind! Hier der Vergleich:

Sonicwall mit vitosecure	Jährlich neue Sonicwall ohne vitosecure
Automatischer Update der Firmware	Manueller Update der Firmware nur innerhalb von 90 Tagen
UTM Dienste (Spyware, Gateway Antivirus, IPS) vorhanden	-
Ersatz der Sonicwall innerhalb von 24h	Ersatz der Sonicwall innerhalb der Garantie (mehrere Tage)
Zentrale Sicherung der Konfiguration; bei einem Defekt kann die Konfiguration jederzeit wiederhergestellt werden	-
Konfigurationsänderungen werden durch Sonicwall zertifizierte Spezialisten durchgeführt	-
Permanente Überwachung der Sonicwall	-

Zusammenfassung: mit dem vitosecure Vertrag bietet die Vitodata AG dem Kunden einen erstklassigen Service an, der auch nicht mit dem ständigen Erwerb eines Neugerätes verglichen werden kann!



Ich habe ein Kombigerät (Router/Firewall), genügt diese Sicherheit nicht? Der Hardwarelieferant meint, diese Sicherheit genüge, da es ja eine Hardwarefirewall ist.

In den meisten Fällen handelt es sich bei diesen Kombigeräten, um sogenannte Zwitter, welche weder Router noch Firewall sind... aber beides ein wenig können! Die Funktionalitäten sind bei diesen, oft sehr günstigen Geräten, äusserst knapp bemessen und können niemals mit den Funktionen einer richtigen Firewall mithalten. Weiter gibt es bei diesen Geräten meistens keine Softwareupdates, keine Erweiterungsmöglichkeiten, keine Konfigurationsmöglichkeiten und somit auch kein umfassender Schutz.

Zusammenfassung: bei Kombigeräten handelt es sich um Zwitter, welche keines wirklich beherrschen, was sich dementsprechend auch im Preis niederschlägt!

Was ist der genaue Leistungsumfang vom vitosecure? Was machen all diese Dienste genau?

Der genaue Leistungsumfang kann im Vertrag selber nachgeschlagen oder in der obenstehenden Tabelle entnommen werden.

Hier eine Beschreibung der Dienste (UTM), welche im Rahmen des vitosecure Vertrages auf der Firewall freigeschalten werden:

- **Echtzeit-Virenprüfung am Gateway (vor dem Eintritt in das Netzwerk):**
Eine leistungsstarke und innovative Methode sorgt für intelligenten Schutz, indem sie Dateien in Echtzeit auf Viren, Würmer, Trojaner und andere Bedrohungen aus dem Internet überprüft.
Vorteil: so können viele Bedrohungen schon vor dem Eintreten in das Netzwerk abgewendet werden!
- **Dynamischer Spyware-Schutz (vor dem Eintritt in das Netzwerk):**
Blockiert die Installation böswilliger Spyware vor dem Eintreten in das Netzwerk und verhindert die unbemerkte Übermittlung vertraulicher Daten durch vorhandene Spyware-Programme.
Vorteil: so wird nicht nur sehr viel Spyware bereits auf der Sonicwall abgewendet, sondern es wird auch versucht bestehender Spyware im Netzwerk den Zugang ins Internet zu vereiteln.



- **Leistungsstarke Intrusion Prevention (vor dem Eintritt in das Netzwerk):** Schützt vor einer Vielzahl von Netzwerk-Bedrohungen auf Anwendungsebene. Downloads werden auf Würmer, Trojaner, Software-Schwachstellen (z. B. Pufferüberläufe, Peer-to-Peer- und Instant Messaging-Anwendungen, Backdoor- Angriffe, Web 2.0) und sonstigen bösartigen Code überprüft. **Vorteil:** heutige Schadsoftware werden immer raffinierter und versuchen sich zu als legitime Software zu tarnen und dies kann am ehesten mit dieser Methode bekämpft werden.

Zusammenfassung: den täglich wechselnden, meist unvorhersehbaren Angriffen kann heutzutage nur noch mit einem Unified Threat Management (UTM) effizient Paroli geboten werden.

Weshalb kann der Global VPN Client nur auf einer Sonicwall und nicht auf einer anderen Firewall eingerichtet werden?

Dies ist ganz einfach eine technische Beschränkung, da der Global VPN Client von Sonicwall so konzipiert wurde, dass er nur mit einer Sonicwall funktionieren kann. Unter anderem wird die Lizenz des Global VPN Client auf der Sonicwall verwaltet und diese Lizenz kann nur auf einer Sonicwall eingelesen werden.

Es gibt jedoch diverse andere VPN Clients anderer Hersteller, welche genau dasselbe wie der Global VPN Client bezwecken. Für die Zywall gibt es z.B. den Zywall IPSec VPN Client.

Zusammenfassung: weil diese eine technische und Hersteller abhängige Einschränkung ist, auf welche wir keinen Einfluss haben.

Weshalb kann allgemein eine VPN Verbindung jeweils nur zwischen zwei Geräte desselben Herstellers eingerichtet werden?

Die faire Antwort auf diese Frage ist: dies ist keine technische Beschränkung, sondern eine rein politische. Was bedeutet das? Grundsätzlich ist es so, dass in der Theorie ein VPN zwischen allen möglichen IPSec fähigen Firewalls (ist heutzutage eigentlich bei allen Firewalls gegeben) aufgebaut werden kann. Die Erfahrung zeigt, dass dies auch zu mehr als 95% der Fälle auch zutrifft. In den wenigen Fällen, in welchen kein VPN aufgebaut werden kann, liegt das Problem entweder beim technischen Verständnis oder an einer exotischen Firewall.

Warum die Vitodata AG generell ein VPN nur zwischen zwei Sonicwalls aufbauen will, ist eine Frage des Aufwands. Die Vitodata AG kann grundsätzlich mit ihrem vorhandenen Know-how ein VPN zwischen jeder möglichen Firewall konfigurieren.



Jedoch ist der Aufwand für eine solche Konfiguration im vornherein sehr schwer abschätzbar, da das spezifische Wissen zu jeder Firewall zuerst angeeignet werden muss. Wenn der Berater sicherheitshalber ca. 2h für die Konfiguration eines VPN's zwischen einer Sonicwall und einer anderen Firewall oder sogar zwischen zwei Nicht-Sonicwalls offerieren würde, dann könnte man dies durchaus auch in Erwägung ziehen... solange es sich um „richtige“ Hardwarefirewalls handelt!

Zusammenfassung: ein VPN kann zwischen unterschiedlichen Herstellern erstellt werden, jedoch bedeutet dies ein bedeutender Mehraufwand und zusätzlich anfallende Kosten!

Warum benötige ich eine fixe IP Adresse, wenn ich von zu Hause auf meine Praxis zugreifen möchte?

Damit der Kunde von zu Hause aus auf Informationen in der Praxis zugreifen kann, muss er ein VPN aufbauen können, damit diese Informationen über eine gesicherte Verbindung übertragen werden. Dies lässt sich am besten mit einem Tunnel vergleichen. Bei einem VPN handelt es sich um einen Tunnel, in welchem die Daten ungesichtet von A nach B gelangen können.

Heute werden fast alle Internetabonnemente ohne fixe IP Adressen vergeben. Das heisst, der Eintrittsknoten (IP Adresse) ins Internet bekommt periodisch immer wieder eine andere IP Adresse. Konkret: die IP Adresse in der Praxis und zu Hause ändert ca. alle 24h einmal. Grund dafür ist die beschränkte Anzahl an momentan verfügbaren IP Adressen weltweit... doch dies ist dann wieder ein Thema für sich.

Um nun einen VPN Tunnel aufbauen zu können, muss mind. der Zielknoten (IP Adresse) zwingend bekannt sein, da ansonsten unklar ist wohin (Ziel) denn nun der VPN Tunnel aufgebaut werden muss. Dies lässt sich am besten mit einem Navigationssystem vergleichen. Man kann nur dann eine Route durch das Navigationssystem planen lassen, wenn einem bekannt ist, wohin es gehen soll. Sobald das Ziel bekannt ist, berechnet das Navigationssystem den Weg dorthin automatisch.

Zusammenfassung: damit eine sichere Verbindung (VPN Tunnel) in die Praxis aufgebaut werden kann, darf die IP Adresse in der Praxis nicht immer wieder ändern und genau dies kann mit einer fixen IP Adresse gelöst werden.