

12. Firewall

Autor: Friedrich Heckmann

Stand: Sept. 2009

Inhaltsverzeichnis

12.Firewall.....	1
12.1.Skalierbarkeit.....	1
12.1.1. Ohne dedizierte Firewall.....	2
12.1.2. Einsatz einer Appliance.....	3
12.2.Konfiguration der Firewall.....	3
12.3.Zusammenfassung.....	5

In der paedML Novell 3 kommt ein völlig überarbeitetes Firewall-Konzept zum Einsatz. Um auch zukünftigen Anforderungen gerecht zu werden, wird als zentraler Punkt eine dedizierte Firewall mit mindestens drei Netzwerkkarten eingesetzt. Über diese ist es nun möglich, physikalisch getrennte Sicherheitszonen wie DMZ und verschiedene Gäste-Netze zu bilden. Der jeweils zulässige Datenverkehr der Zonen kann so zentral gesteuert werden. Die notwendige Hardware für die Firewall kann je nach Schultyp und dem zu erwartenden Datenaufkommen frei skaliert werden.

Die dargestellten WEB-Services, die unter OES1 auf einer UML liefen, können in der paedML3.2 unter OES2 auf dem OES-Server selbst oder auf einer separaten Hardware betrieben werden. Vergl. hierzu Kap. 10 Webdienste.

12.1. Skalierbarkeit

Die Bandbreite der Skalierbarkeit reicht vom Betrieb ohne dedizierte Firewall mit Zugriff über BelWue-Router bis hin zur größten Ausbaustufe mit dem Einsatz einer Appliance (ASG). Eine mittlere Ausbaustufe stellt die Installation der Software auf einem „Standard-PC“ mit nicht allzu hohen Anforderungen dar. Nähere Einzelheiten siehe Installationsanleitung und Dokumentation von Astaro.

Die folgenden beiden Kapitel beschreiben die prinzipiellen Funktionen der kleinsten und größten Ausbaustufen.

Die Schulen können im Prinzip auch eine Firewall ihrer Wahl einsetzen, welche die notwendigen Funktionalitäten aufweist. Das Support-Netz des LMZ kann in diesem Fall aber keinerlei Unterstützung und Support zur Firewall bieten.

Aus diesem Grunde empfehlen wir ausdrücklich beim Einsatz einer Firewall mindes-



tens die Variante des ASL als Firewall zu verwenden, welche mit dem Erwerb der paedML Novell 3 ausgeliefert wird. Die Firewallsoftware wird von der Firma Astaro kostenlos zur Verfügung gestellt und kann auf geeigneter Hardware installiert werden.

Diese Version mit einer speziellen Schullizenz, welche beim LMZ geordert werden muss, ist auf den hauptsächlichen Einsatz in der paedML Novell 3 abgestimmt. Dies sowohl in einer Einschulllösung als auch in einer Mehrschulunggebung mit einem oder mehreren Servern, welche über VPN-Kanäle über eine WAN-Verbindung kommunizieren müssen. Hier kommen dann die Vorzüge der Astaro Security Linux (ASL) oder gegebenenfalls einer Astaro Security Gateway Appliance (ASG), besonders zum Tragen.

In beiden Varianten (Software und Hardware) ist der Bereich *Network Protection* mit Firewall, VPN und Intrusion Prevention voll lizenziert. Bei der kostenfreien ASL-Variante ist jedoch die maximale Verbindungszahl auf 50 IP-Adressen begrenzt, was aber für die paedML Novell 3 keine Einschränkung darstellt, da die Verbindung zwischen Server und Firewall über eine einzige IP abgebildet wird.

Die ASG-Varianten besitzen diesbezüglich keine Einschränkungen.

12.1.1. Ohne dedizierte Firewall

Wird vom Kunden auf die neuen zusätzlichen Funktionalitäten der ML3, wie z.B. die sichere Anbindung von WLAN- und Gäste-Netzen, verzichtet, so ist es auch möglich, die Anbindung des Schulnetzes an das Internet ohne eigene Firewall, direkt über den BelWue-Router, zu betreiben. Die Konfiguration des BelWue-Routers mit seinen Filterlisten wird hierbei von BelWue selbst übernommen.

Bedingt durch die Realisierung der Internetsperre auf dem Gserver03 geht selbst bei dieser minimalen Konfiguration keinerlei Funktionalität gegenüber der ML2.x verloren. Sie wurde in ihrer Wirkung sogar noch effizienter.

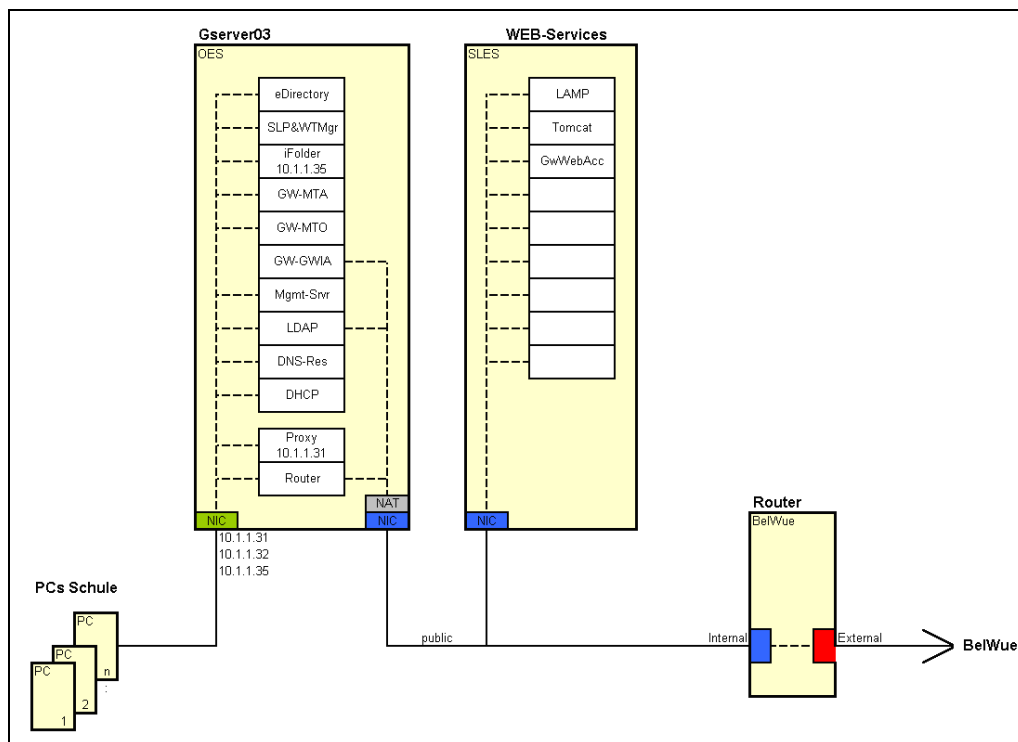


Abbildung 12.1.: paedML Novell 3.0 ohne Firewall

12.1.2. Einsatz einer Appliance

Den vollen Funktionsumfang der Firewallfunktionalität stellt die Astaro Security Gateway Appliance (ASG) dar. Diese vorkonfigurierte Hardware-Variante lässt keine Wünsche mehr offen. Sie kann zu besonderen Konditionen erworben werden.

Bei Bedarf können von der Schule optionale Komponenten wie *Web Filtering* (inhaltsbasierte Filter, Anti-Virus, Anti-Spyware und IM/P2P-Kontrolle), *Email Security* (Anti-Spam, Anti-Virus und Anti-Phishing) sowie *Email Encryption* gebucht werden. Diese Funktionalitäten gehen aber weit über die Grundfunktionalitäten einer einfachen schulischen Firewall hinaus und verursachen demzufolge auch zusätzliche Folgekosten. Größere Installationen mit mehr als 40 Gäste-PCs und / oder WLAN-PCs sollten eine Investition in eine Appliance (ASG) in Erwägung ziehen. Diese wird generell mit einer Gold Maintenance (GM) geliefert.

Die Gold Maintenance bedeutet 24h Reaktionszeit bei Defekten und gegebenenfalls Austausch der Hardware!

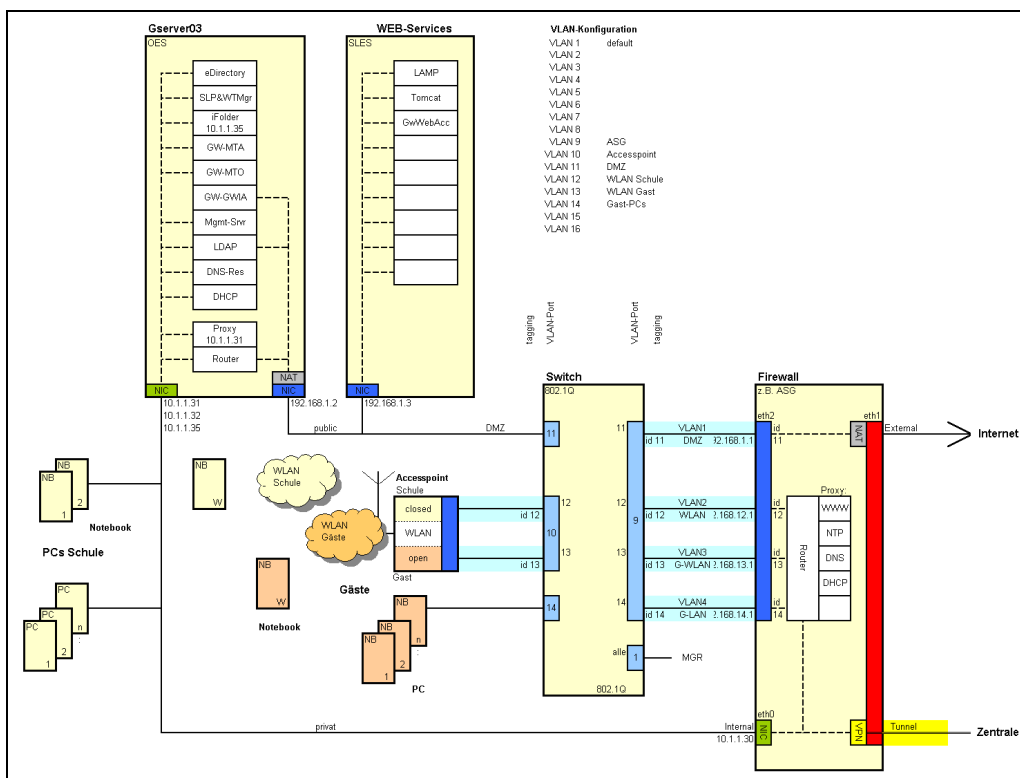


Abbildung 12.2.: paedML Novell 3.0 mit Firewall

12.2. Konfiguration der Firewall

Die Firewall kann über ein Web-Interface mittels Browser konfiguriert werden. Der Zugang ist passwortgeschützt unter der Adresse <https://10.1.1.30:4444> zu erreichen.



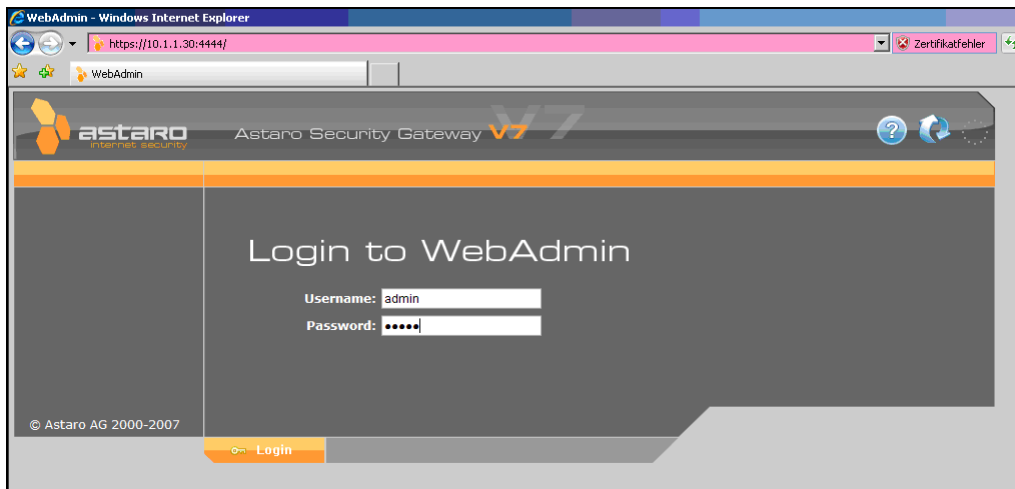


Abbildung 12.3.: Astaro WebAccess-Anmeldung

Die übersichtliche Oberfläche erlaubt alle Arten der Konfiguration, sowie ein einfaches Sichern und Rücksichern der gesamten Konfiguration.

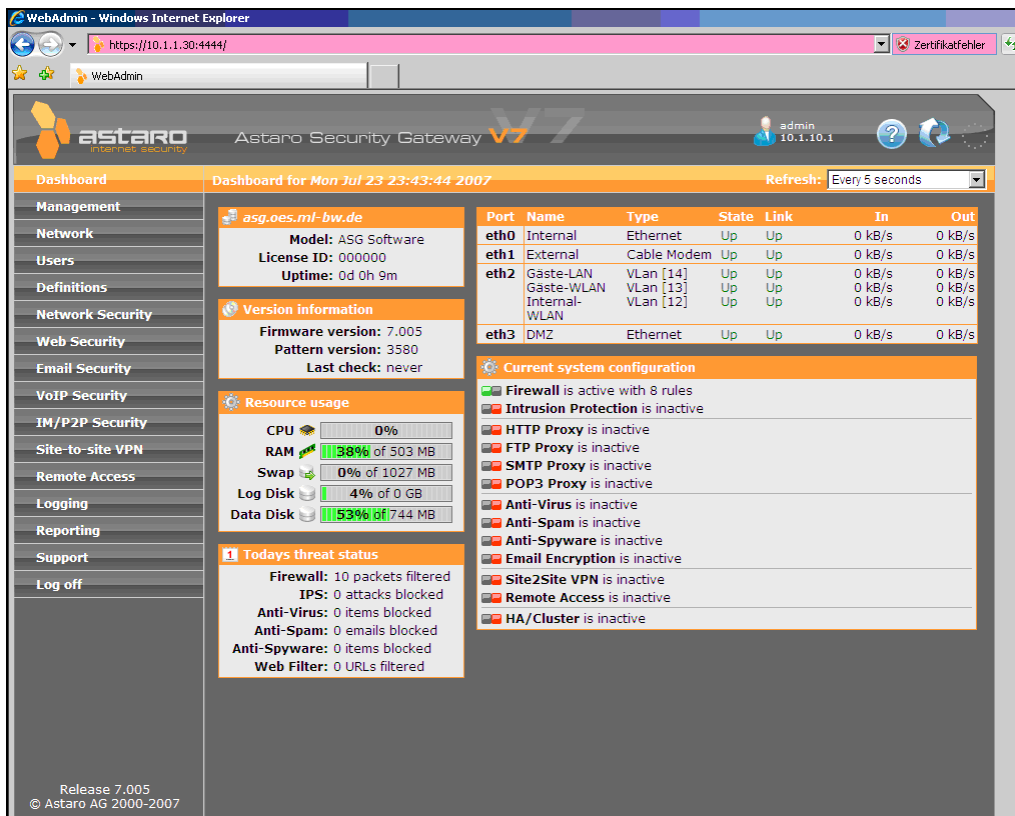


Abbildung 12.4.: Astaro WebAccess

Nähere Einzelheiten siehe Dokumentation der paedML Novell 3.0.

12.3. Zusammenfassung

Folgende Merkmale zeichnen die Firewall in der paedML Novell 3.0 aus:

- Die Variante der Firewall kann von der Schule frei gewählt werden.
- Es stehen von der kostenlosen bis zur kostenpflichtigen Variante mit vollem Funktionsumfang mehrere Varianten zur Wahl.
- Die Installation ist dokumentiert und die Konfiguration vorbereitet.
- Die Konfiguration ist auf den schulischen Einsatz abgestimmt.
- Die Firewall stammt aus dem professionellen Umfeld, sodass qualifizierte Händler mit ihrem Umgang vertraut sind.
- Bei Gold Maintenance:
24h Reaktionszeit bei Defekten und ggf. Austausch der Hardware.