

Summary

Version 10.01.2005

Diplomarbeit I00 (2004)

MuSeGa

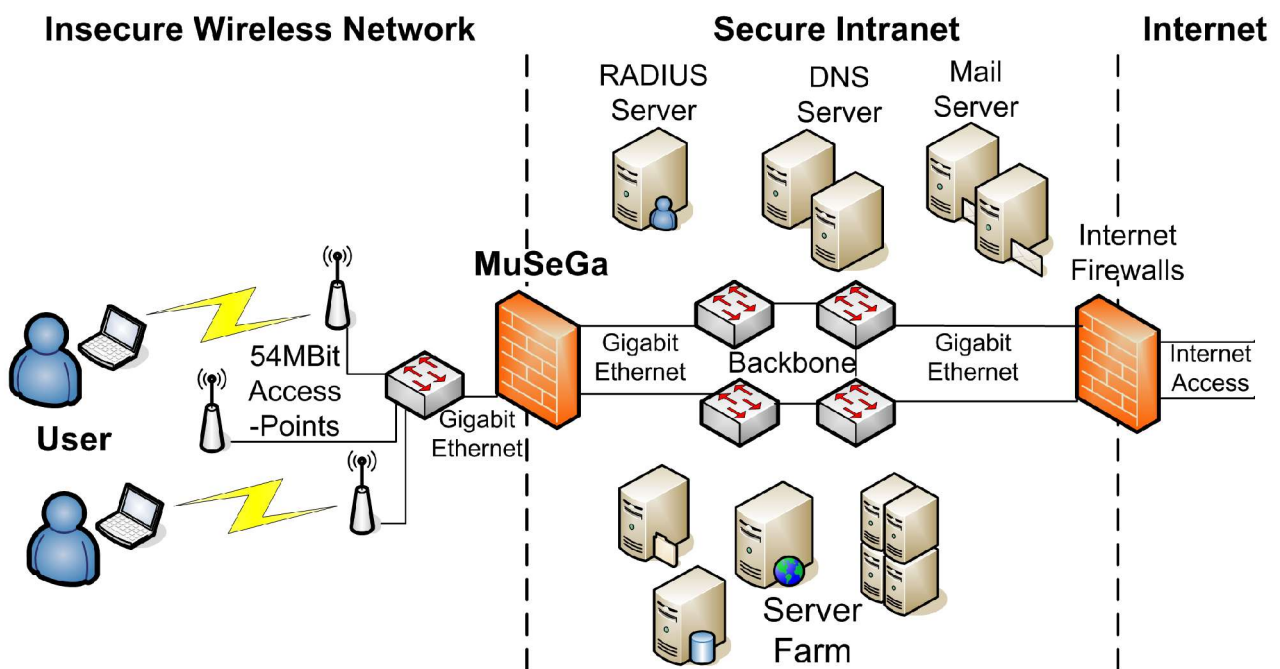


Mobile User Secure Gateway

Experte: Andreas Dürsteler (Swisscom)
Betreuer: Hansjürg Wenger (HTI)
Gerhard Hassenstein (HTI)
Diplomand: Lukas Reusser (Swisscom)

Abstract

Wireless-Netzwerke werden immer beliebter. So auch an der Hochschule für Technik und Informatik in Bern. Diese stellt ihren Studenten, Mitarbeitern und Dozenten einen Wireless-Zugang zu ihrem Netzwerk zur Verfügung. Um den Zugangsschutz zu gewährleisten, wird momentan eine Lösung von Bluesocket eingesetzt. Diese Bluesocket-Box stösst aber schon bald an ihre Leistungsgrenze, da das Wireless-Netzwerk in naher Zukunft auf den neuen 54Mbit Standard (IEEE 802.11g) umgerüstet wird. Leistungsstärkere Hardware von Bluesocket oder auch von anderen Herstellern sind teuer. Hier kommt MuSeGa ins Spiel. Mit leistungsstarker PC-Hardware und Opensource-Software wurde eine eigene Lösung für den gesicherten Zugang zum Hochschulnetz entwickelt. MuSeGa wird später evtl. an der ganzen BFH eingesetzt.



(Abbildung 001, MuSeGa Übersicht)



Was MuSeGa alles kann

MuSeGa basiert auf Debian Linux 3.1 und bietet folgende Funktionalitäten:

- Stateful Firewall (mit Objekt orientierter Konfiguration)
- NAT/NAPT Support
- Detailliertes Bandwidth Management (Benutzer oder Firewall-Objekt basierend)
- Authentifizierung lokal sowie via RADIUS
- VLAN Support
- DHCP Server
- DNS Forwarding
- SMTP Catch and Forwarding (Mails versenden ohne Client umzukonfigurieren)
- PPTP Endpunkt mit MPPE Verschlüsselung, MPPC Komprimierung und MSCHAP-V2
- Detaillierte Traffic Statistiken (pro Benutzer, pro Dienst sowie der gesamte Verkehr)
- Administration via Web-GUI
- MAC Blacklist (zum aussperren von unerwünschten Clients)
- MAC History (zum wieder auffinden verschwundener Hardware)
- SWITCHmobile kompatibel
- Automatischer SWITCHmobile ACL Generator
- Misconduct Detection (ermöglicht das Aussperren von Clients mit Viren/Würmer etc.)
- ...

Funktionsweise

Die Funktionsweise lässt sich kurz wie folgt beschreiben: Per Standardeinstellung wird der gesamte Netzwerkverkehr, der vom Wireless-Netzwerk her kommt, gelöscht. Eine Ausnahme bildet hier nur der Web-Verkehr, der auf die Loginseite auf dem MuSeGa umgeleitet wird. Der Client bezieht also vom Gateway via DHCP eine Adresse und wird auf die Loginseite umgeleitet. Dort gibt er nun seinen Benutzernamen und sein Passwort ein, welche via RADIUS Server überprüft werden. Waren die Angaben korrekt, liefert der RADIUS Server ein Attribut zurück, welches die Zuteilung des Benutzers in eine lokale Gruppe zulässt. Anhand der für diese Gruppe gespeicherten Berechtigungen werden nun Firewall-Regeln generiert und auf die IP- und MAC-Adresse des Clients appliziert. Der Client kann nun auf alle für ihn vorgesehenen Ressourcen zugreifen. Loggt sich ein Benutzer manuell aus, oder macht sein PC eine gewisse Zeit kein DHCP-Renew, werden alle zu diesem Client gehörenden Regeln wieder gelöscht. Die komplette Administration vom Mobile User Secure Gateway wird über ein Web-Interface vorgenommen. Es können verschiedene Statistiken sowie das Benutzerverhalten abgefragt werden. Die gesamte Konfiguration ist in einer Datenbank gespeichert. Somit ist ein Import/Export sehr leicht möglich und auch das Backup ist abgedeckt. Bei der Implementation wurde speziell darauf geachtet, dass für die einzelnen Funktionalitäten nur bewährte und weit verbreitete Softwarepakete eingesetzt wurden. Dies hat den Vorteil, dass man stets mit Updates und Security-Patches versorgt wird und man den Gateway so auf einem aktuellen und sicheren Stand halten kann.