





**Sicherheitslücke SSL –
Traffic Vortrag 1M07**

Bernhard Graf adARTIS e.K.



Wer ist adARTIS ?

- adARTIS e.K.
- Gegründet 1991
- Geschäftsführer Bernhard Graf
- 8 Mitarbeiter
- 2 Lotus Notes CLPs
- 1 IBM certified eBusiness Instructor
- IBM Advanced Business Partner
- UNIX Projekte und Produkte von Anbeginn
- Partner von Bull, IBM, Sun
- Lotus Notes seit 1998
- Security Produkte seit 2001



Unsere Leistungen

- Security Beratung
 - E-Mail Security - JULIA Mailoffice
 - Web-Security - TOMMY SSL-Proxy
 - Virenscanner - TrendMicro, AntiVir
- OpenSource Beratung
 - CMS - TYPO3
 - eLearning - Moodle
 - Groupware - eGroupware
 - File- und Printservices PC -Samba
 - File- und Printservices Mac - NetAtalk
 - openLDAP
 - squid
 - ...
- eBusiness Beratung
 - Lotus Notes
 - IBM WebSphere
 - IBM SecureWay LDAP



Ausgangslage

SSL ("Secure Socket Layer"):
bei SSL - z.B. zum sicheren Übertragen von
Kreditkarteninformationen -
wird zwischen den beiden Endpunkten (i.d.R. ein Browser und
ein Internet-Host) verschlüsselt.



The diagram shows a green laptop icon labeled 'Clients' on the left and a globe icon labeled 'Internet' on the right. In the center is a blue padlock icon labeled 'https'. Dashed double-headed arrows connect the laptop to the padlock, and the padlock to the globe, representing the secure communication channel.


Problem

Bei einer "Ende-zu-Ende"-Verschlüsselung ist zentraler Virenschutz (Inhaltsschutz) somit unterbunden und ausschließlich auf dem Client möglich.

- hoher Aufwand = hohe Kosten oder
- Sicherheitsrisiko
- Beispiel : `http://webmailer.hosteurope.de` erkennt Viren in heruntergeladenen Mails aber `https://webmailer.hosteurope.de` erlaubt das Herunterladen sämtlicher Virenmails !!!

Weiterhin ist die bei SSL-Serverseiten die Prüfung von Zertifikaten notwendig.
Diese wird i.d.R. am Client vorgenommen.

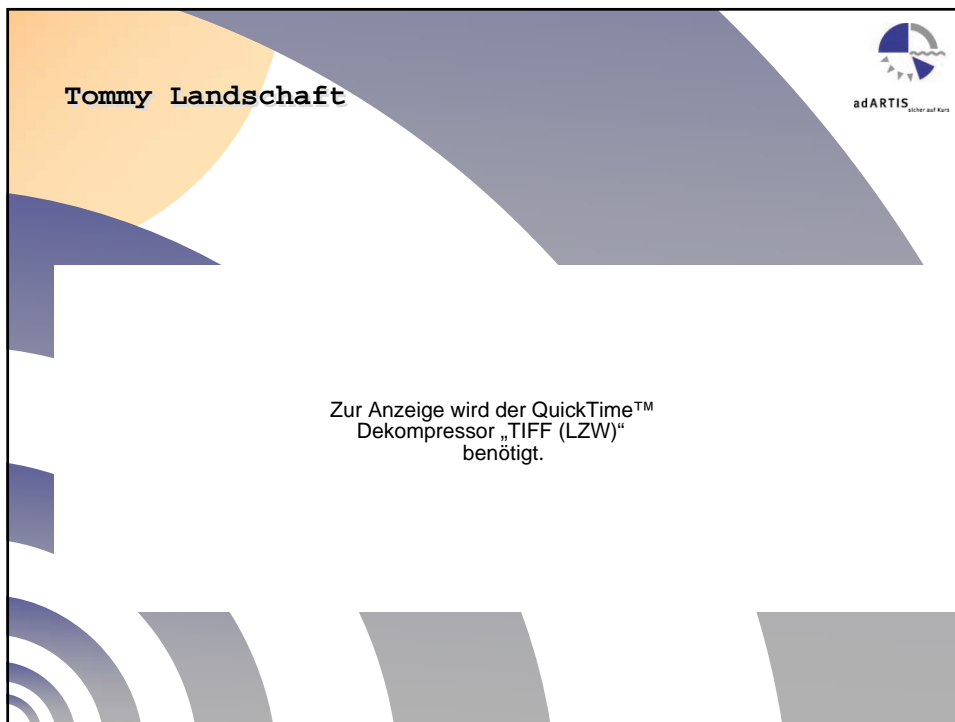
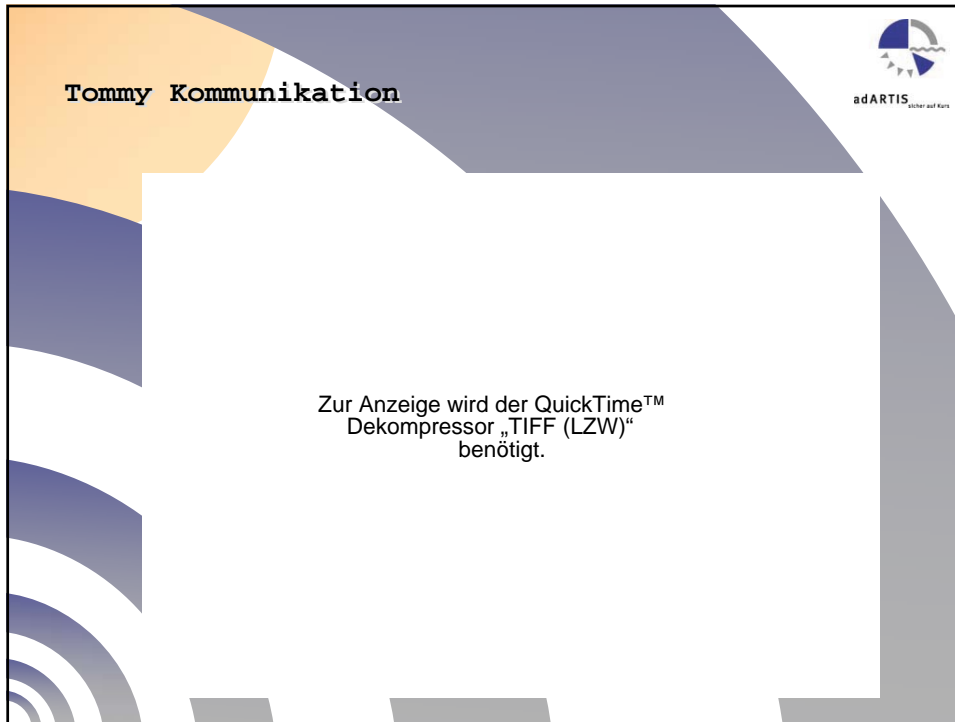
- hoher Aufwand = hohe Kosten
- Client wird mit einbezogen




Lösung

- TOMMY ermöglicht die zentrale Inhaltssicherung des SSL-Datenstroms
- TOMMY kontrolliert zentral die Serverzertifikate der SSL-Server und hält zentral Client-Zertifikate für die Authentisierung bereit








Multithreaded Tommy Architektur


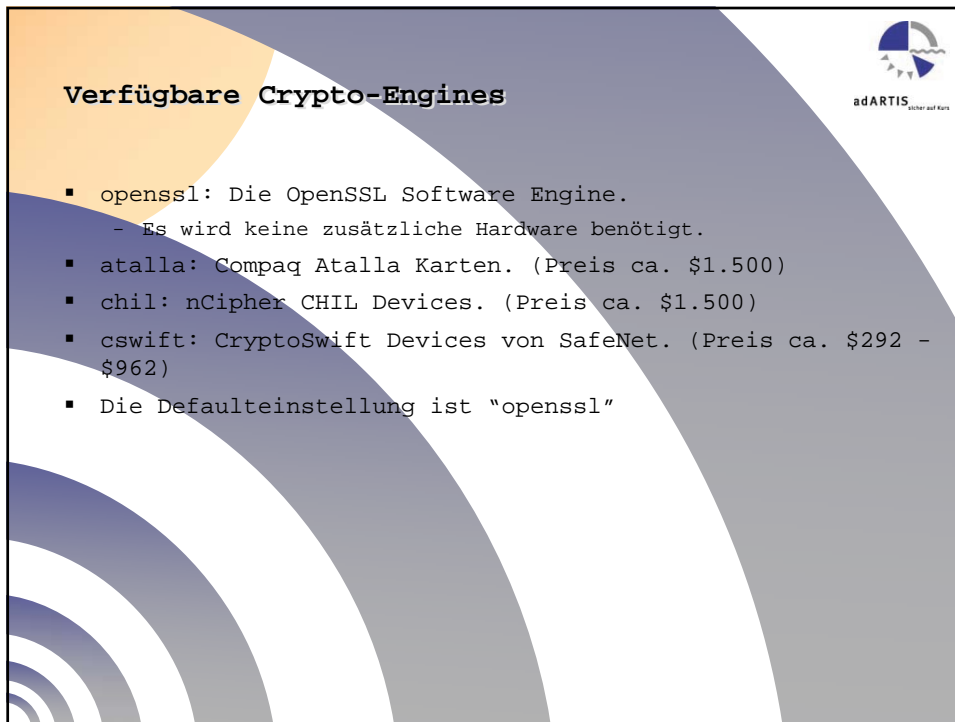
- Authentifizierung durch squid Proxy
- Virenscannung durch Trendmicro Scanner
- Weg ist : squid -> tommy1 (https-http Wandlung)
-> trendmicro -> tommy2 -> (http-https Wandlung) -> Zielserver
- Und wieder retour

Zur Anzeige wird der QuickTime™ Dekompressor „TIFF (LZW)“ benötigt.




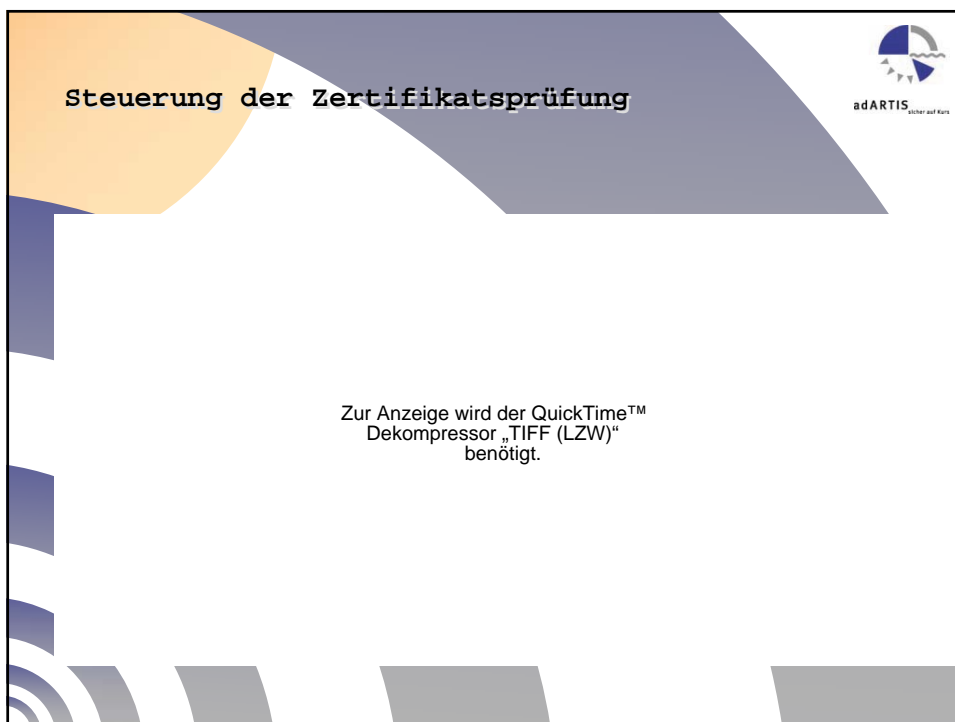
Layered Architektur

Tommy SSL Proxy
WEB-Frontend
Konfiguration
Open SSL Bibliothek
TOMMY-Kern-Programm
Squid (optional)
Linux/Solaris/AIX



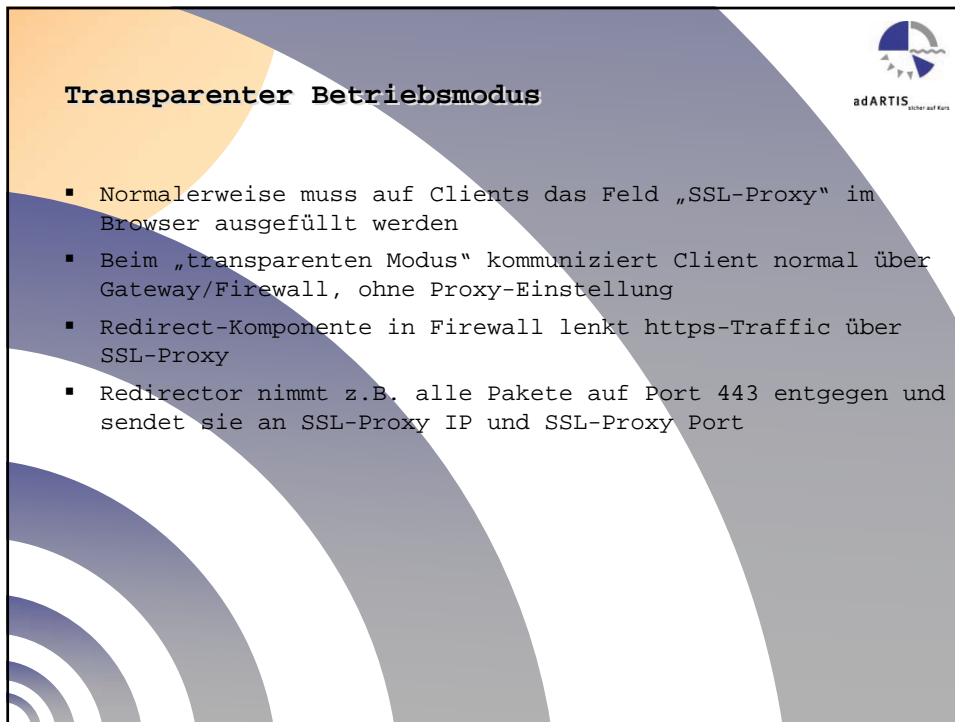
Verfügbare Crypto-Engines

- openssl: Die OpenSSL Software Engine.
 - Es wird keine zusätzliche Hardware benötigt.
- atalla: Compaq Atalla Karten. (Preis ca. \$1.500)
- chil: nCipher CHIL Devices. (Preis ca. \$1.500)
- cswift: CryptoSwift Devices von SafeNet. (Preis ca. \$292 - \$962)
- Die Defaulteinstellung ist "openssl"



Steuerung der Zertifikatsprüfung

Zur Anzeige wird der QuickTime™ Dekompressor „TIFF (LZW)“ benötigt.




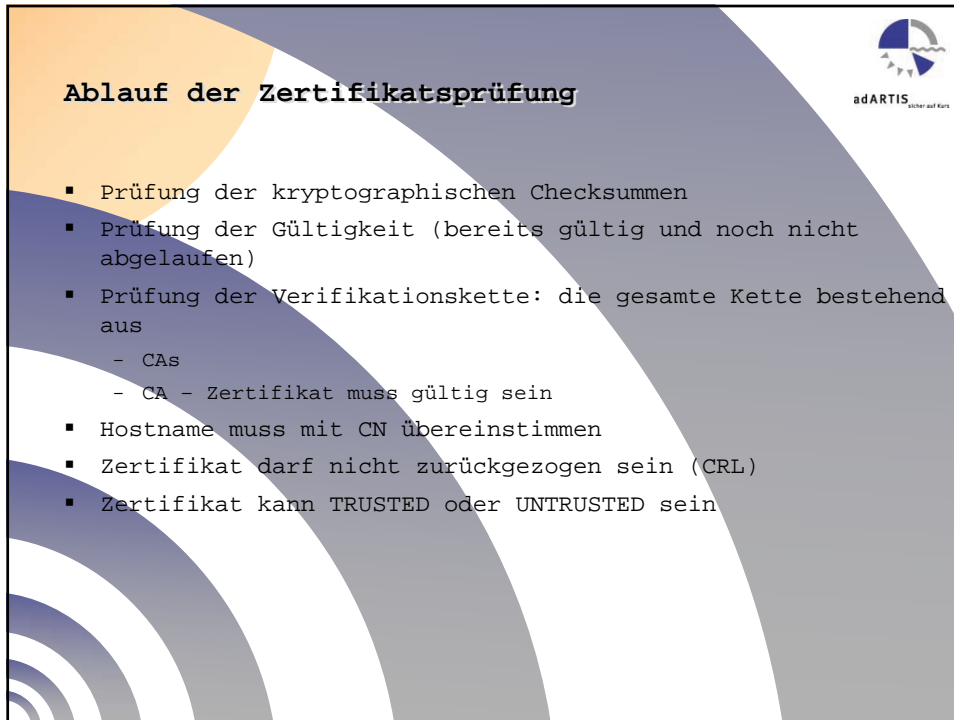
Transparenter Betriebsmodus

- Normalerweise muss auf Clients das Feld „SSL-Proxy“ im Browser ausgefüllt werden
- Beim „transparenten Modus“ kommuniziert Client normal über Gateway/Firewall, ohne Proxy-Einstellung
- Redirect-Komponente in Firewall lenkt https-Traffic über SSL-Proxy
- Redirector nimmt z.B. alle Pakete auf Port 443 entgegen und sendet sie an SSL-Proxy IP und SSL-Proxy Port




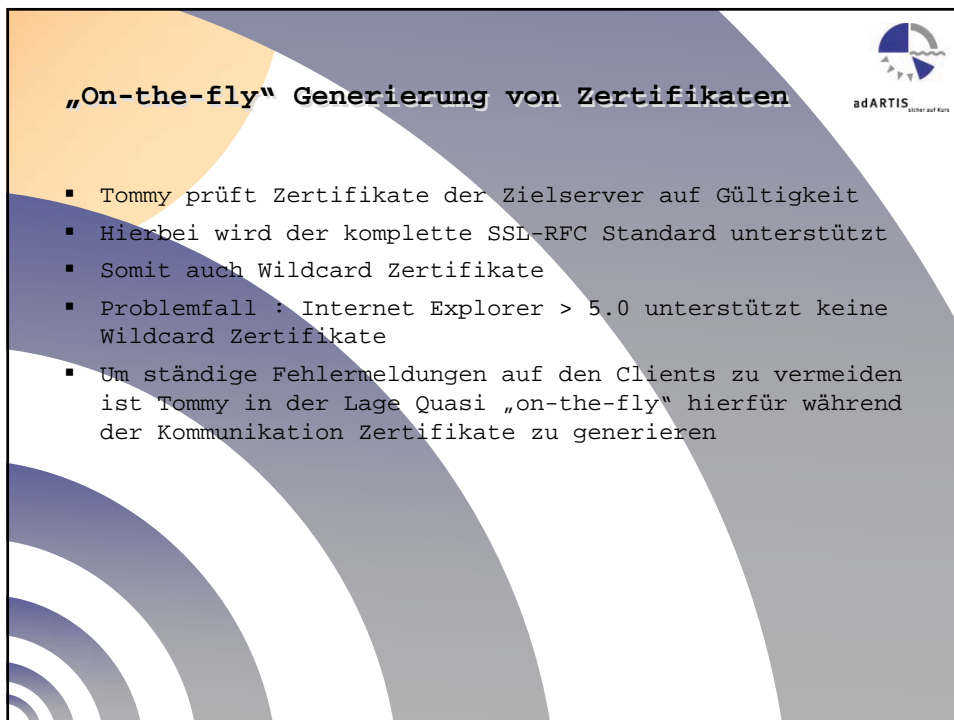
Zertifikats-Optionen

Zur Anzeige wird der QuickTime™ Dekompressor „TIFF (LZW)“ benötigt.




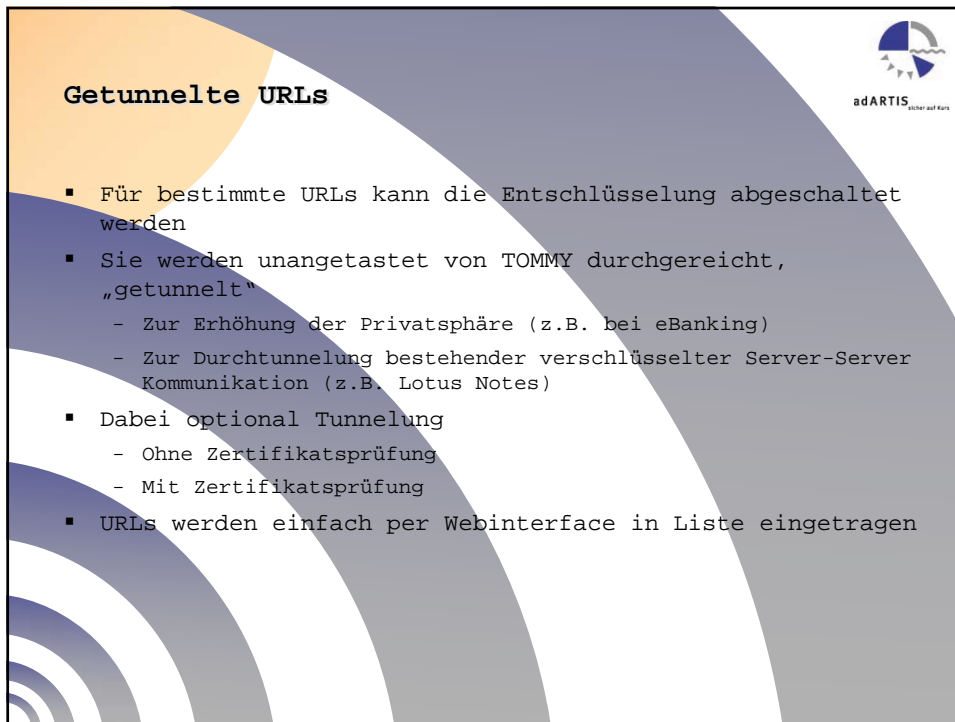
Ablauf der Zertifikatsprüfung

- Prüfung der kryptographischen Checksummen
- Prüfung der Gültigkeit (bereits gültig und noch nicht abgelaufen)
- Prüfung der Verifikationskette: die gesamte Kette bestehend aus
 - CAs
 - CA - Zertifikat muss gültig sein
- Hostname muss mit CN übereinstimmen
- Zertifikat darf nicht zurückgezogen sein (CRL)
- Zertifikat kann TRUSTED oder UNTRUSTED sein




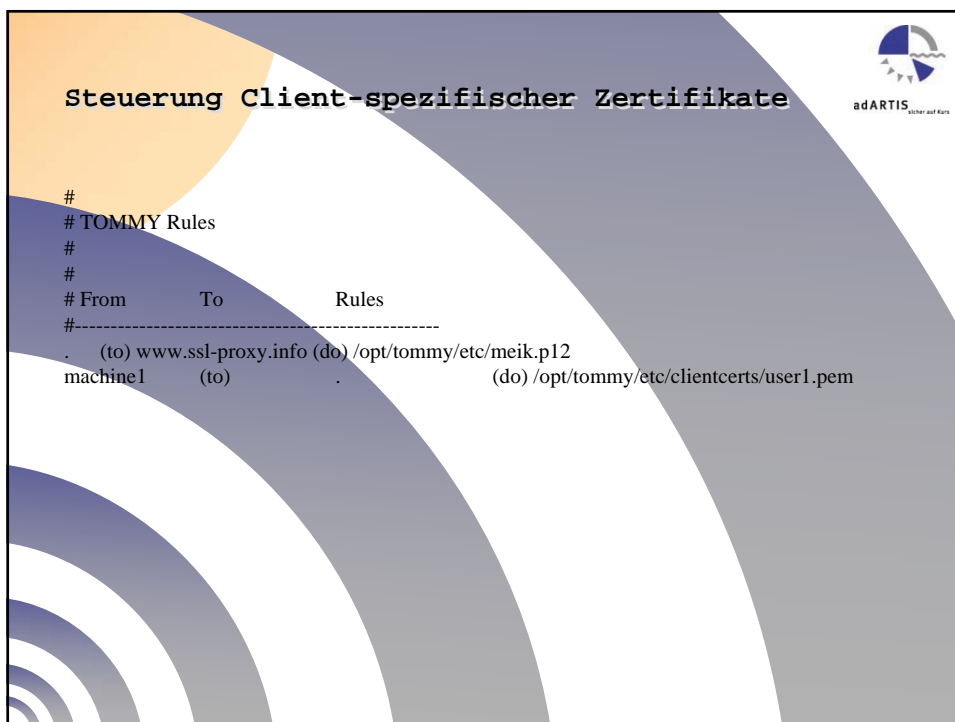
„On-the-fly“ Generierung von Zertifikaten

- Tommy prüft Zertifikate der Zielseverer auf Gültigkeit
- Hierbei wird der komplette SSL-RFC Standard unterstützt
- Somit auch Wildcard Zertifikate
- Problemfall : Internet Explorer > 5.0 unterstützt keine Wildcard Zertifikate
- Um ständige Fehlermeldungen auf den Clients zu vermeiden ist Tommy in der Lage Quasi „on-the-fly“ hierfür während der Kommunikation Zertifikate zu generieren



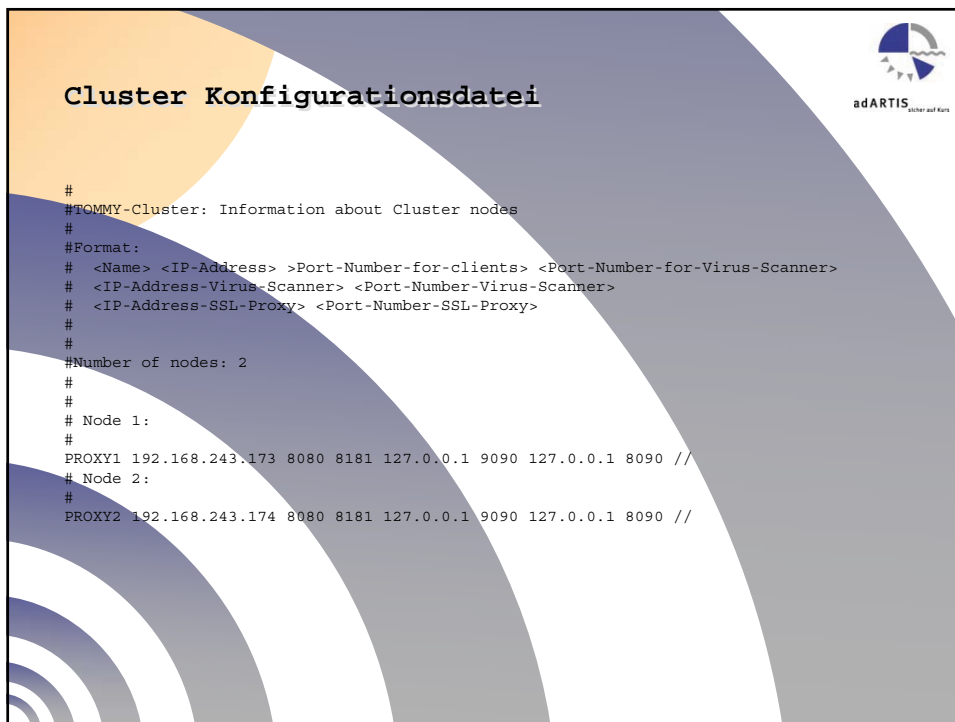
Getunnelte URLs


- Für bestimmte URLs kann die Entschlüsselung abgeschaltet werden
- Sie werden unangetastet von TOMMY durchgereicht, „getunnelt“
 - Zur Erhöhung der Privatsphäre (z.B. bei eBanking)
 - Zur Durchtunnelung bestehender verschlüsselter Server-Server Kommunikation (z.B. Lotus Notes)
- Dabei optional Tunnelung
 - Ohne Zertifikatsprüfung
 - Mit Zertifikatsprüfung
- URLs werden einfach per Webinterface in Liste eingetragen



Steuerung Client-spezifischer Zertifikate


```
#  
# TOMMY Rules  
#  
#  
# From      To      Rules  
#-----  
. (to) www.ssl-proxy.info (do) /opt/tommy/etc/meik.p12  
machine1 (to) . (do) /opt/tommy/etc/clientcerts/user1.pem
```





Technische Voraussetzungen

- SOLARIS Version 8 oder 9
 - Sun Ultrasparc 5
 - 256 MB RAM
 - 3 GB Festplatte
- LINUX ab glibc-Version 2.2
 - Pentium III, 700 MHZ
 - 256 MB RAM
 - 3 GB Festplatte
- AIX ab Version 4.3.3
 - ab RS/6000 B50 oder 150
 - 256 MB RAM
 - 3 GB Festplatte



Vorteile von TOMMY SSL-Proxy

- Flexibilität - TOMMY ermöglicht den Einsatz beliebiger proxy-basierter Sicherheitssysteme
- Nahtlose Integration in bestehende Umgebungen (z.B. Proxy-Ketten)
- Server- und Clientauthentisierung
- Skalierbare Anpassung an steigenden Leistungsbedarf
- Keine neue Software auf den Clients notwendig
- Keine Löcher mehr in der Firewall

Rechtliche Hinweise - Betriebsvereinbarung



- Es gibt oftmals rechtliche Bedenken beim Einsatz eines SSL-Proxies
- Wenn Mitarbeitern privates Browsen erlaubt ist, stellt das Entschlüsseln und Scannen des SSL-Traffics einen Eingriff in die Privatsphäre dar
- Dies kann durch explizites Erwähnen im Rahmen einer Betriebsvereinbarung rechtssicher gemacht werden
- Alternativ kann das private Browsen untersagt werden

Anwender (Auszug)



- AXA-Versicherungen
- BSI - Bundesamt f. Sicherheit i. d. Informati te
- DBV Winterthur
- DEVK Versicherung
- DZ-Bank
- End Armaturen, Bad Oeynhausen
- Flughafen Köln-Bonn GmbH
- Gothaer Versicherung
- ivv - Informationsverarbeitung für Versicherungen GmbH
- KfW Kreditanstalt für Wiederaufbau
- Signal-Iduna-Versicherung
- Vattenfall Europe AG





Ansprechpartner

Vielen Dank für Ihre Aufmerksamkeit!

Bernhard Graf

Tel.: 06439 / 9123-0
Mobil: 0172-9745449
E-Mail: bgraf@adartis.de
Web: www.adartis.de

 adARTIS
über auf Kurs