

Testbericht iSecure

Dokumenten-Nr.
Version 0.1 – Stand 25.03.2003

- nur für den internen Gebrauch - Entwurf-

Version 1.1 (Stand 25. März 2003)

Dieses Dokument ist nur gültig, wenn sein Stand mit dem unter:

http://spuinfo.intranet.commerzbank.com/invsv_regelw/default.htm

genannten Stand übereinstimmt.

©Copyright Commerzbank Aktiengesellschaft 2000

Herausgeber:

Commerzbank Aktiengesellschaft
Standardisierungsbereich DV
60261 Frankfurt am Main

Geltungsbereich:

Autor: Gerd Gruhn, SCOPE Consulting GmbH

Dieses Dokument wurde mit Microsoft Word für Windows 97 erstellt.

Inhaltsverzeichnis

1	Vorbemerkungen	1
2	Testaufbau	2
2.1	Hardwarekonfiguration	3
2.2	Softwarekonfiguration	4
3	Durchgeführte Tests	5
3.1	DoS-Attacken	5
3.1.1	DoS-Attacke auf Norton Personal Firewall mit zwischengeschaltetem iSecure	5
3.1.1.1	Volle Bandbreite	5
3.1.1.2	Modem-Bandbreite	5
3.1.2	DoS-Attacke auf Norton Personal Firewall ohne zwischengeschaltetem iSecure	5
3.1.2.1	Volle Bandbreite	5
3.1.2.2	Modem-Bandbreite	6
3.1.3	DoS-Attacke auf Firewall One mit zwischengeschaltetem iSecure	6
3.1.3.1	Volle Bandbreite	6
3.1.3.2	Modem-Bandbreite	6
3.1.4	DoS-Attacke auf Firewall One ohne zwischengeschalteten iSecure	6
3.1.4.1	Volle Bandbreite	6
3.1.4.2	Modem-Bandbreite	6
3.2	Netzwerkfunktionalität	6
3.2.1	http	6
3.2.2	ftp	6
3.2.3	telnet	6
3.2.4	Microsoft-Netzwerk	7
3.3	Datendurchsatz	7
4	Testergebnisse	8
4.1	DoS-Attacken	8
4.1.1	DoS-Attacke auf Norton Personal Firewall mit zwischengeschaltetem iSecure	8
4.1.1.1	Volle Bandbreite	8
4.1.1.2	Modem-Bandbreite	8
4.1.2	DoS-Attacke auf Norton Personal Firewall ohne zwischengeschaltetem iSecure	8
4.1.2.1	Volle Bandbreite	8
4.1.2.2	Modem-Bandbreite	9
4.1.3	DoS-Attacke auf Firewall One mit zwischengeschaltetem iSecure	9
4.1.3.1	Volle Bandbreite	9
4.1.3.2	Modem-Bandbreite	9
4.1.4	DoS-Attacke auf Firewall One ohne zwischengeschalteten iSecure	9
4.1.4.1	Volle Bandbreite	10
4.1.4.2	Modem-Bandbreite	10
4.2	Netzwerkfunktionalität	10
4.2.1	http	10
4.2.2	ftp	10
4.2.3	telnet	10
4.2.4	Microsoft-Netzwerk	10
4.3	Datendurchsatz	10
5	Zusammenfassung	11

Änderungsnachweis

Version 0.1

Februar 2001

Gerd Gruhn

Freigabe durch den Prüfer

Freigabe durch den Verantwortlichen

Verzeichnis der Abbildungen

Abbildung 1, Testkonfiguration mit iSecure	2
Abbildung 2, Testkonfiguration ohne iSecure	3

Verzeichnis der Tabellen

Tabelle 1, Aufgaben der Testsysteme	2
Tabelle 2, Hardwarekonfiguration der Testsysteme	3
Tabelle 3, Softwarekonfiguration der Testumgebung	4

1 Vorbemerkungen

In jüngster Zeit häufen sich Angriffe gegen Computersysteme in öffentlichen und privaten Netzen. Dabei spielt zunehmend eine Technik eine Rolle, welche als DoS (**D**eny **o**f **S**ervice) und dDoS (**d**istributed **D**eny **o**f **S**ervice) bezeichnet wird. Diese Techniken zielen darauf ab, gezielt einzelne Services eines Systems zu stören oder zum Erlegen zu bringen. Dies kann dem Ziel dienen, durch gezielte Ausnutzung von Unzulänglichkeiten an den angegriffenen Systemen Zugang zu diesen zu erhalten oder diese Angriffe werden mit dem Ziel gestartet, bestimmte Rechner oder Netzwerke als solche lahm zu legen.

Die Problematik bei derartigen Angriffen liegt darin, dass die heute verfügbaren Firewalls keinen oder nur sehr eingeschränkten Schutz gegen solche Angriffe bieten. Bereits verfügbare Softwareprodukte sind höchstens geeignet sehr kleine Netzwerke mit einer schmalbandigen Netzwerkanbindung vor derartigen Angriffen zu schützen.

Mit dem Produkt **iSecure** der Firma SCOPE Consulting GmbH wurde uns ein Produkt zum Test angeboten, welches DoS- und dDoS-Angriffe blockieren soll.

Das vorliegende Dokument beschreibt den dazu verwendeten Testaufbau, die durchgeführten Tests, sowie die ermittelten Testergebnisse. In der Zusammenfassung werden Einsatzmöglichkeiten bei der Commerzbank AG diskutiert.

2 Testaufbau

Die folgenden Grafik zeigt den Testaufbau mit zwischengeschaltetem iSecure:

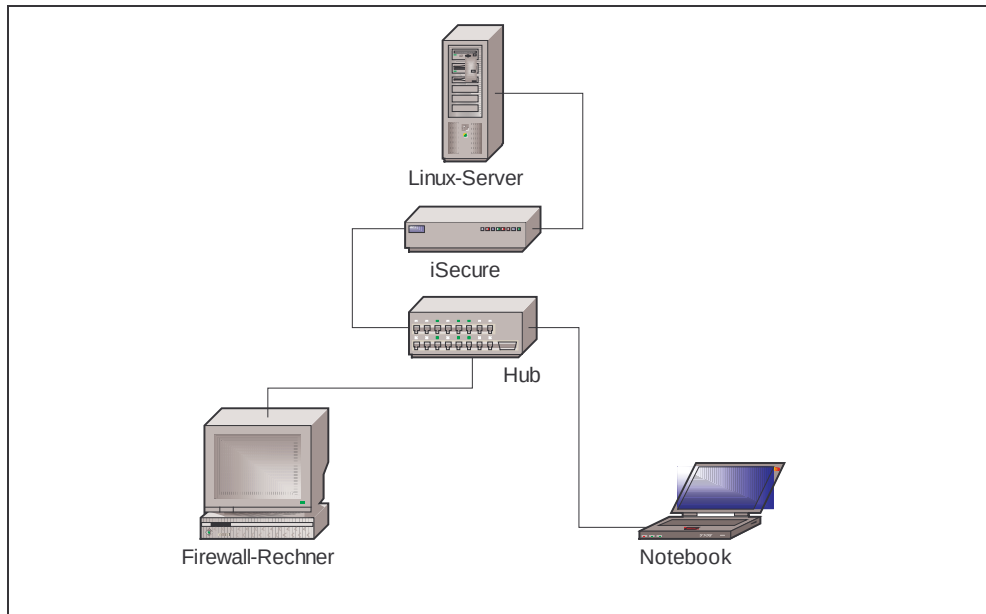


Abbildung 1, Testkonfiguration mit iSecure

Diese Testkonfiguration dient für folgende Tests:

- DoS-Angriffe auf den Firewall mit zwischengeschaltetem iSecure.
- Kontrolle der Verfügbarkeit der wichtigsten Netzwerkdienste mit zwischengeschaltetem iSecure.
- Messung des Datendurchsatzes mit zwischengeschaltetem iSecure.

Die folgende Tabelle gibt einen Überblick über die Aufgaben der einzelnen Systeme:

Tabelle 1, Aufgaben der Testsysteme

System	Aufgabe
Linux-Server	• Angriffsrechner • Webserver • MS-Netzwerk-Server (Samba) • telnet-Server • ftp-Server
Hub	• Herstellung der Netzwerkverbindungen
Firewall-Rechner	• angegriffener Rechner • Webserver • Windows NT-Server • telnet-Server • ftp-Server • Netzwerkmonitoring • Firewall-Server
Notebook	• Netzwerkmonitoring

Die folgende Abbildung zeigt den Testaufbau ohne iSecure.

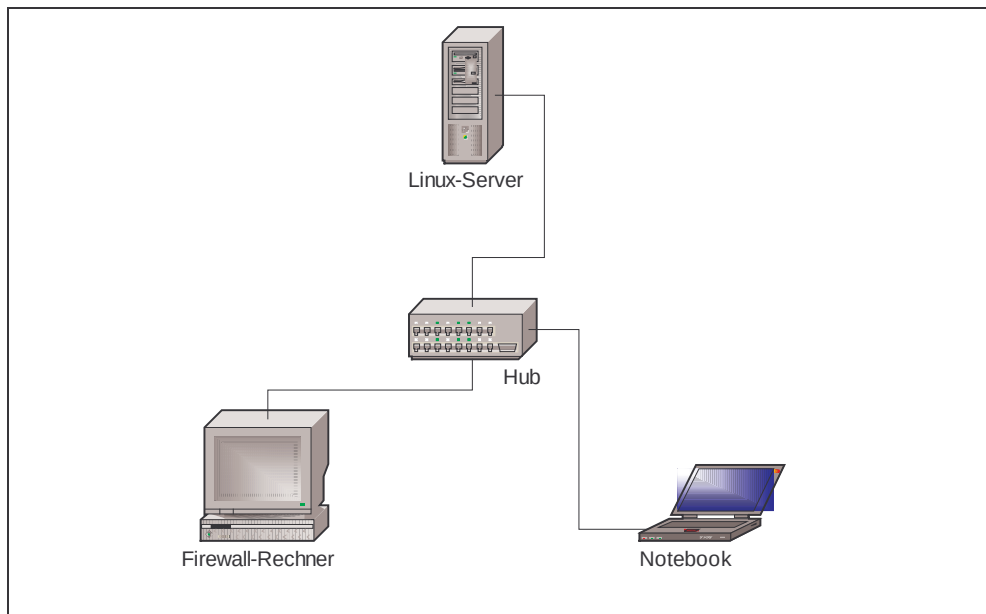


Abbildung 2, Testkonfiguration ohne iSecure

Dieser Testaufbau wird bei den folgenden Tests verwendet:

- DoS-Angriffe ohne zwischengeschaltetem iSecure.
- Messung des Datendurchsatzes ohne zwischengeschaltetem iSecure.

Die Netzwerkverbindung basiert durchgängig auf 10 MBit Ethernet.

2.1 Hardwarekonfiguration

Die folgende Tabelle gibt einen Überblick über den für den Test relevanten Hardwareausbau der verwendeten Systeme:

Tabelle 2, Hardwarekonfiguration der Testsysteme

System	Komponenten
Linux-Server	• 2 x Pentium 90 • 64 MByte RAM • 10 / 100 MBit Ethernetkarte
HUB	• HP-Ethernet-HUB 10 MBit/s
Firewall-Rechner	• Pentium II 200 • 64 MByte RAM • 10 / 100 Ethernetkarte
Notebook	• AMD Athlon 700 • 64 MByte RAM • 10 / 100 PCMCIA Ethernetkarte

2.2 Softwarekonfiguration

Die folgende Tabelle gibt einen Überblick über die für den Test relevante Softwarekonfiguration:

Tabelle 3, Softwarekonfiguration der Testumgebung

System	Softwarekomponenten
Linux-Server	• SuSE-Linux 7.0 (Erstinstallation ohne Updates) • datapool 3 (Sammlung von DoS-Attacken)
Hub	• keine Softwarekomponenten vorhanden
Firewall-Rechner	• Windows NT 4.0, SP 4 • Norton Personal Firewall 2000
Notebook	• Windows 2000 Professional, SP 1 • Exceed 6.0

Das Tool datapool 3 beinhaltet die folgenden DoS-Attacken:

ADMdnsfuckr, akill2.pl, arnup100, ascend-foo, beer, biffit, binds, bloop, bncex, boink, bonk, cocksuck, coke, comatose, conseal, d0s.pl, DoS-Linux.pl, dos-prox.pl, DoS_frontpage.pl, duy, echok, fawx, flatline, flushot, foqerc, galt_gin, gewse, gewse5, gin, hanson, hell, hestra, hiperbomb2, inetd.DoS, ircd_kill, jaypee, jolt, killwin, kill_inetd, kkill, koc, kod, kox, land, laser, latierra, linux-icmp, locktcp, mailer, misfrag, mmsu-dos, moyari13, mutilate, nestea, nestea2, newtear, nt-dns, octopus, opentear, orgasm, oshare_1_gou, overdrop, paralyze3, pepsi, pimp, pimp2, pirchslap, pong, quake2, rape, raped, rc8, rcon, rpk, rucm, rwhokill, simping, slice3, smack, spender.pl, spiffit, sprite, ssping, stealth, stream, syndrop, synful, synhose, synk, synk4, targa, targa2, targa3, teardrop, tesoiis, trash, trash2, twinge, udpdata, udpflood, winfreez, wingatecrash und winnuke.

3 Durchgeführte Tests

Dieses Kapitel beschreibt die durchgeführten Tests. Angriffe gegen eine Firewall One konnten noch nicht getestet werden, da die dazu benötigten Lizenzen noch nicht verfügbar sind.

3.1 DoS-Attacken

Die DoS-Attacken wurden mit dem Tool datapool 3 durchgeführt. Ziel der Tests war die Überprüfung, ob iSecure angegriffene Systeme zuverlässig schützen kann. Dazu werden DoS-Angriffe auf den Firewall-Rechner mit und ohne Schutz gefahren. Zusätzlich werden die Angriffe mit voller Bandbreite und mit der Bandbreite eines 56k-Modems gefahren um die typischen Situationen abzudecken.

Als permanente Kontrolle wird vom Notebook permanent ein Ping auf das angreifende und das angegriffene System abgesetzt, um deren Verfügbarkeit zu prüfen. Das angegriffene System (Firewall-Rechner) setzt permanent einen Ping auf sein lokales Netzwerkinterface ab, um dessen Verfügbarkeit zu prüfen.

3.1.1 DoS-Attacke auf Norton Personal Firewall mit zwischengeschaltetem i-Secure

3.1.1.1 Volle Bandbreite

Dieser Test verwendet datapool 3 bei Nutzung der vollen Netzwerk-Bandbreite als Angriffstool auf den Firewall-Rechner. Der Notebook testet mit einem permanenten Ping die Verfügbarkeit des Firewall-Rechners und des angreifenden Linux-Servers. Auf dem Firewall-Rechner wird mit einem Ping auf das lokale Netzwerkinterface dessen Verfügbarkeit überprüft. Zur Kontrolle, ob einzelne Pakete aus DoS-Angriffen den Firewall-Rechner erreichen wird die Norton Personal Firewall im Monitoring-Mode gestartet.

Ziel des Testes ist der Nachweis, dass iSecure den Firewall-Rechner zuverlässig gegen DoS-Attacken schützt.

3.1.1.2 Modem-Bandbreite

Dieser Test entspricht dem Test aus Gliederungspunkt 3.1.1.1 mit dem Unterschied, dass für die Angriffe eine Netzwerkbandbreite von 56 kBit verwendet wird.

3.1.2 DoS-Attacke auf Norton Personal Firewall ohne zwischengeschaltetem iSecure

3.1.2.1 Volle Bandbreite

Bei diesem Test geht es darum, nachzuweisen, dass DoS-Attacken ohne zwischengeschaltetem iSecure zur Blockierung und Funktionsstörung der angegriffenen Rechner führen. Er ist also die Gegenprobe zu den Tests aus Gliederungspunkt 3.1.1.

Zu diesem Zweck wird mit datapool 3 vom Linux-Server aus ein Angriff auf den Firewall-Rechner mit voller Netzwerkbandbreite gefahren. Der Notebook kontrolliert wiederum die Verfügbarkeit an Angriffsrechner und Firewall-Rechner mit einem permanenten Ping. Auf dem Firewall-Rechner wird ebenfalls eine permanente Ping auf das lokale Netzwerkinterface zur Kontrolle von dessen Verfügbarkeit gestartet. Um die Angriffe zu protokollieren wird auf dem angegriffenen Rechner die Norton Personal Firewall gestartet. In einem zweiten Test wird die Norton Personal Firewall nicht gestartet, um zu kontrollieren, wie lange der angegriffene Rechner ohne Firewall verfügbar bleibt.

3.1.2.2 Modem-Bandbreite

Dieser Test entspricht dem Test aus Gliederungspunkt 3.1.2.1. Der Unterschied besteht in der verwendeten Netzwerkbandbreite von 56 kBit.

3.1.3 DoS-Attacke auf Firewall One mit zwischengeschaltetem iSecure

Diese Tests werden durchgeführt, sobald eine Lizenz für eine Firewall One verfügbar ist.

3.1.3.1 Volle Bandbreite

3.1.3.2 Modem-Bandbreite

3.1.4 DoS-Attacke auf Firewall One ohne zwischengeschalteten iSecure

Diese Tests werden durchgeführt, sobald eine Lizenz für eine Firewall One verfügbar ist.

3.1.4.1 Volle Bandbreite

3.1.4.2 Modem-Bandbreite

3.2 Netzwerkfunktionalität

Ziel der Tests in diesem Kapitel ist die Kontrolle der Verfügbarkeit der wichtigsten Netzwerkprotokolle bei zwischengeschaltetem iSecure. Dabei wird die Funktionalität zum einen vom Linux-Server hin zur Firewall und umgekehrt geprüft.

3.2.1 http

Ziel des Testes ist die Kontrolle, ob das http-Protokoll über iSecure hinweg funktioniert.

Webserver auf dem Linux-Server ist ein Apache-Webserver. Webserver auf dem Firewall-Rechner ist ein IIS.

Als Client kommt auf dem Webserver ein Netscape 4.7- und auf dem Firewall-Rechner ein Internetexplorer 5.0 zum Einsatz.

Getestet wird der Aufruf einer Apache-HTML-Seite vom Firewall-Rechner aus und der Aufruf einer IIS-HTML-Seite vom Linux-Server aus.

3.2.2 ftp

Dieser Test dient der Kontrolle, dass ftp-Verkehr über iSecure hinweg möglich ist.

Als ftp-Server- und Client dienen jeweils der Linux-Server und der Firewall-Rechner.

Getestet wird der Transfer eines Files vom Linux-Server auf den Firewall-Rechner und umgekehrt.

3.2.3 telnet

Mit diesem Test wird überprüft, ob telnet-Sessions über iSecure hinweg möglich sind.

Auf Linux-Seite wird der mitgelieferte telnet-Demon und telnet-Client. Auf der Seite vom Firewall-Rechner kommt der telnet-Demon von Exceed 6 und der telnet-Client von Windows NT 4.0 zum Einsatz.

Der Test besteht darin, vom Linux-Server auf eine telnet-Session auf dem Firewall-Rechner- und vom Firewall-Rechner eine Telnet-Session auf dem Linux-Server zu starten.

3.2.4 Microsoft-Netzwerk

Bei diesem Test wird überprüft, ob Verbindungen über das smb-Protokoll über iSecure hinweg möglich sind.

Als smb-Server auf Linux-Seite kommt der mit SuSE 7.0 mitgelieferte Samba-Server zum Einsatz. Als smb-Client dienen die Programme smbclnt und smbmount. Auf der Seite des Firewall-Rechners kommen die Standardfunktionen von Windows NT 4.0 zum Einsatz.

Folgende Tests werden jeweils in Richtung Linux zu Windows NT und umgekehrt durchgeführt:

- Browsen des Netzwerkes nach smb-Servern.
- Aufbau einer smb-Netzwerkverbindung.

3.3 Datendurchsatz

Der letzte Test soll feststellen, inwieweit sich der Datendurchsatz mit und ohne iSecure ändert.

Dazu werden von Windows NT auf Linux per Microsoft-Netzwerk-Verbindung 7 Files mit insgesamt 70.352.896 Bytes mit und ohne zwischengeschaltetem iSecure transferiert. Die dazu benötigte Zeit wird gemessen.

4 Testergebnisse

4.1 DoS-Attacken

4.1.1 DoS-Attacke auf Norton Personal Firewall mit zwischengeschaltetem iSecure

4.1.1.1 Volle Bandbreite

Der Windows NT-Rechner überstand den Angriff unbeschadet. Zeitweise waren weder der Firewall-Rechner als auch der Linux-Server nicht per Ping erreichbar. Dies ist in der vollen Ausnutzung der Netzwerkbandbreite begründet und stellt keine Fehlfunktion von iSecure dar.

Von den 106 DoS-Angriffen konnte keiner den Windows NT-Rechner erreichen. Lediglich bei vier Angriffen konnten einzelne Datenpakete aus DoS-Attacken iSecure passieren. Diese Datenpakete stellten aber keinen vollständigen Angriff dar (keine Erkennung durch Firewall) und belegten nur ca. 5 % der Netzwerkbandbreite. Dabei handelte es sich um Datenpakete aus folgenden Angriffen:

- fawx,
- oshare_1_gou,
- stuffit und
- ADMdnsfuckr.

Nach dem Ende der Angriffe waren sowohl der Firewall-Rechner als auch der Linux-Rechner voll im Netzwerk erreichbar.

Während der Angriffe war das Interface des Firewall-Rechners ständig erreichbar.

iSecure hat also das hinter ihm liegende Netz zuverlässig gegen die DoS-Angriffe geschützt.

4.1.1.2 Modem-Bandbreite

Das Ergebnis unterschied sich erwartungsgemäß nicht vom Ergebnis des vorherigen Tests. Einziger Unterschied war, dass wegen der verwendeten geringeren Netzwerkbandbreite sowohl der angreifende Linux-Server als auch der Firewall-Rechner ständig erreichbar waren. Damit konnte nachgewiesen werden dass bei einem DoS-Angriff die Kommunikation zwischen den voreinander geschützten Netzen weiterhin möglich ist, wenn genügend Bandbreite zur Verfügung steht. iSecure filtert also selektiv Datenpakete aus DoS-Attacken heraus.

4.1.2 DoS-Attacke auf Norton Personal Firewall ohne zwischengeschaltetem iSecure

4.1.2.1 Volle Bandbreite

Durch die DoS-Attacken ohne zwischengeschaltetem iSecure war das Netzwerkinterface des Angreifenden Rechners nur teilweise und das des Firewall-Rechners überhaupt nicht erreichbar. Die Ursache liegt hierbei in der vollen Ausnutzung der Netzwerkbandbreite durch die Tests und die Angriffe selbst.

Die Angriffe führten nicht zum Absturz des Windows NT-Rechners, wohl aber zum Ausfall seiner gesamten Netzwerkfunktionalität. Er war nach den Angriffen sowohl bei aktivierter Firewall als auch bei

deaktivierter Firewall nicht mehr über das Netzwerk erreichbar und konnte auch selbst von keinem anderen Rechner mehr erreicht werden.

Das Windows NT-Netzwerk wurde erst nach einem Umstellen der Netzwerkgeschwindigkeit im Kartentreiber von 10 auf 100 MBit und wieder zurück verfügbar.

Die folgenden gemessenen Zeiten bis zum Ausfall des Windows NT-Netzwerkinterfaces beziehen sich auf den Zeitpunkt des Ausfalls des Pings des Firewall-Rechners auf seine lokale Netzwerkkarte.

- Ausfall mit aktiver Firewall: 15:23 Minuten.
- Ausfall ohne aktiver Firewall: 10:25 Minuten.

Somit konnte nachgewiesen werden, dass DoS-Angriffe auf nicht mit iSecure geschützte Rechner zum Ausfall der Systeme führen, auch wenn sie durch eine Firewall geschützt werden. Da der Ausfall des Netzwerkes schon auf Treiberebene erfolgt, ist auch eine Firewall kein Schutz gegen DoS-Angriffe, da sie erst die Datenpakete entgegennimmt, die der Treiber liefert. Mit einem Ausfall des Treibers der Netzwerkkarte fällt also auch die Firewall aus.

4.1.2.2 Modem-Bandbreite

Die Ergebnisse bei diesem Test decken sich im wesentlichen mit denen des vorherigen Tests. Daher wird hier nur auf die Unterschiede eingegangen.

Der Linux-Server war während der Angriffe permanent erreichbar. Der Firewall-Rechner war nur sporadisch erreichbar. Von je ca. 50 Pings wurde einer beantwortet.

Die gemessenen Zeiten bis zum Ausfall des Netzwerkes des Firewall-Rechners sind:

- mit aktiver Firewall 23:47 Minuten und
- ohne aktiver Firewall 17:27 Minuten.

Dieser Test hat gezeigt, dass ein einzelner angreifender Rechner mit einem Modem am Internet angeschlossen ausreicht, um einen Rechner mit DoS-Angriffen außer Betrieb zu setzen.

4.1.3 DoS-Attacke auf Firewall One mit zwischengeschaltetem iSecure

Diese Tests werden durchgeführt, sobald eine Lizenz für eine Firewall ONE verfügbar ist.

4.1.3.1 Volle Bandbreite

4.1.3.2 Modem-Bandbreite

4.1.4 DoS-Attacke auf Firewall One ohne zwischengeschalteten iSecure

Diese Tests werden durchgeführt, sobald eine Lizenz für eine Firewall ONE verfügbar ist.

4.1.4.1 Volle Bandbreite

4.1.4.2 Modem-Bandbreite

4.2 Netzwerkfunktionalität

4.2.1 http

Die Nutzung von http ist mit einem zwischengeschalteten iSecure ohne Einschränkungen und bidirektional möglich.

4.2.2 ftp

Die Nutzung von ftp ist mit einem zwischengeschalteten iSecure ohne Einschränkungen und bidirektional möglich.

4.2.3 telnet

Die Nutzung von telnet ist mit einem zwischengeschalteten iSecure ohne Einschränkungen und bidirektional möglich.

4.2.4 Microsoft-Netzwerk

Die Nutzung des Microsoft-Netzwerkes ist mit einem zwischengeschalteten iSecure ohne Einschränkungen und bidirektional möglich.

4.3 Datendurchsatz

Die Zeit zur Übertragung der Daten ohne iSecure betrug 01:39:60 Minuten und mit zwischengeschalteten iSecure 01:40:13 Minuten.

Da die Zeiten per Hand gestoppt worden sind, liegt der Geschwindigkeitsunterschied nahezu im Bereich der Messtoleranzen.

Eine deutliche Reduzierung der Netzwerkbandbreite durch iSecure kann also nicht festgestellt werden. Der Einsatz von iSecure wird keinen „Flaschenhals“ im Netzwerk erzeugen. Gegen die Reduzierung der Bandbreite beim Einsatz von Firewalls im Netzwerk fällt die Bandbreitenreduzierung durch iSecure nicht mehr ins Gewicht.

5 Zusammenfassung

iSecure schützt Netzwerke zuverlässig gegen DoS-Attacken. Da Firewall-Rechner nahezu unwirksam gegen DoS-Attacken sind und diesen auch weitgehend schutzlos ausgeliefert sind, ist iSecure ein wichtiger und notwendiger Bestandteil jeder Firewallinstallation.

Die Installation von iSecure ist einfach, da nur die Netzwerkinterfaces mit den entsprechenden Anschlüssen zu verbinden sind. Administrativer Aufwand entsteht nicht, da iSecure fertig konfiguriert geliefert wird.

Da iSecure keine eigenen IP-Adressen besitzt, ist es auch nicht angreifbar. Bei allen Angriffen hat iSecure zuverlässig funktioniert. Fehler traten nicht auf.

Da iSecure den Angreifern vortäuscht, dass alle Netzwerkports offen seien, ist es für Angreifer sehr schwierig Schwachstellen im Netzwerk ausfindig zu machen.

iSecure ist als Einschub in 19"-Rack ausgeführt und ist damit in die vorhandenen Racks einfach zu integrieren.

Ein Display, welches im Prototypen noch nicht enthalten war, ermöglicht die visuelle Erkennung von DoS-Attacken.