IPv6 Protokoll-Tests mit der Cisco ASA-5510 (IDSv6)

Simon Kiertscher
Institute of Computer Science
University of Potsdam
14482 Potsdam, Germany
kiertscher@cs.uni-potsdam.de

22. Januar 2014

1 Versuchsaufbau und Konfiguration

Wie in der Vorhabenbeschreibung in Arbeitspaket 4.5 festgehalten, wurden Protokolltests an einer Cisco Firewall durchgeführt. Verwendet wurde die Cisco Adaptive Security Appliance (ASA) 5510 [**?**], welche über ein extra *Intrusion Prevention System* (IPS) verfügt. Cisco ASA 5500 beschreibt dabei die gesamte Produktlinie, die Cisco an Geräten für Netzwerksicherheit führt.

Der Testaufbau sieht vor, dass 2 Maschinen getrennt durch die Firewall versuchen miteinander zu kommunizieren. Hierfür wird das in Arbeitspaket 2.2 entwickelte Autotester-Tool `ft6` (*Firewall Tester für IPv6*) verwendet. Das Tool kann auf der Projektseite unter `http://www.idsv6.de/de/material.html` heruntergeladen werden.

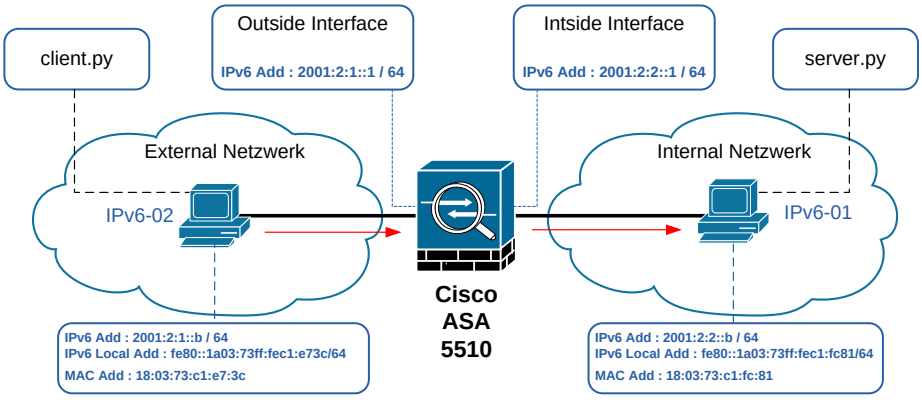

Abbildung 1: Test Setup

Abbildung 1 zeigt den Versuchsaufbau detailliert. Auf der Client-Maschine (IPv6-02) läuft der Client-Teil (`client.py`) von `ft6`, welcher abhängig vom jeweiligen Test, verschiedene Pakete durch die Firewall an den Server (IPv6-01) sendet, auf welchem der Server-Teil (`server.py`) von `ft6` läuft. Der Server sendet dann wiederum an den Client, welche der gesendeten Pakete er empfangen hat, so dass der Client eine Auswertung vornehmen kann.

Es wird dabei über Port 80 kommuniziert, welcher den einzigen offenen Port in der Firewall darstellt. Damit wird ein typischer Webserver Use-Case betrachtet, da Port 80 unter die *well-known* Ports fällt und vom *Hypertext Transfer Protocol* (HTTP) genutzt wird.

Desweiteren wurde die Client-Maschine mit dem als Outside konfigurierten Interface verbunden (niedriges Sicherheitniveau) und die Server-Maschine mit dem als Inside konfiguriertem (hohes Sicherheitniveau). Hierdurch wird sichergestellt, dass keine Kommunikation von Außen nach Innen (Client $\rightarrow$ Server) stattfinden kann (Ausnahme Port 80), wenn nicht bereits eine Verbindung besteht, die vom Server aufgebaut wurde.

Die verwendeten Maschinen nutzen Linux grml 3.7.1-grml-amd64 Debian 3.7.9 + grml.1 x86_64 (uname -a) und auf der ASA läuft der Cisco ASA Software Release Version 9.0(2) mit Cisco Adaptive Security Manager Version 7.1(2).

Alle Tests wurden zweimal durchgeführt. Der erste Test (Basis-Test) hat dabei keine weiteren Regeln für die Firewall eingetragen und es ist auch keine IPS Konfiguration vorgenommen worden. Dabei handelt es sich also um einen *Out-of-the-Box* Test (bis auf die Port 80 Konfiguration). Der zweite Test (Erweiterter-Test) hingegen nutzt Access Rules, Service Policies, etc. oder IPS, um die Tests möglichst erfolgreich durchzuführen. Am Ende von jedem Test wird dessen Ausgang noch einmal Tabellarisch zusammengefasst.

2 ICMPv6 Filtering

RFC 4890 [**?**] beschäftigt sich mit Empfehlungen zur Filterung von ICMPv6 Nachrichten. Daraus resultierend müssen 25 ICMPv6-Typen gefiltert werden, bei 226 ist die Filterung optional und 6 Typen dürfen nicht gefiltert werden.

Basis-Test:

- Von den 25 zu filternden Typen werden 25 (100%) korrekt gefiltert und kein Paket fälschlicherweise weitergeleitet.
- Von den 226 optionalen Typen werden 226 (100%) gefiltert.
- Von den 7 Paketen (6 Typen wobei Typ 4 mit Code 1 und 2 getestet wird), die nicht gefiltert werden sollten, werden 7 (100%) fälschlicherweise gefiltert.

Erweiterter-Test:
Es können durch das Erzeugen von *service-objects* entsprechende ICMPv6 Typen explizit verboten oder erlaubt werden. Diese können auch nach Typen unterschieden werden. Mit dem manuellen Eintragen von Regeln mit diesen *service-objects* kann das Verhalten weiter verbessert werden. Es werden dann bis auf Destination Unreachable (Typ

1), Packet Too Big (Typ 2), Time Exceeded (Typ 3, Code 0) und Parameter Problem (Typ 4, Code 1 & 2) alle Pakete korrekt geblockt bzw. weitergeleitet. Die 4 erwähnten Typen werden trotz expliziter Weiterleitungsregel geblockt. Dieses Verhalten könnte daran liegen, dass es sich bei den 4 Typen um Antworten auf erhaltene Pakete handelt. Da es aber keine vorherigen Pakete gab, auf die geantwortet wird, könnte die Firewall die Pakete deshalb, trotz Regel, blocken.

Tabelle 1 fasst die ICMPv6 Testergebnisse zusammen.

ICPMv6 Pakete	FW-Konfiguration	Wurde Blockiert	Wurde Weitergeleitet
Blockieren	Basis	25 (100%) korrekt	0 (0%) inkorrekt
	Erweitert	25 (100%) korrekt	0 (0%) inkorrekt
Optional	Basis	226 (100%)	0 (0%)
	Erweitert	226 (100%)	0 (0%)
Weiterleiten	Basis	7 (100%) inkorrekt	0 (0%) korrekt
	Erweitert	5 (71%) inkorrekt	2 (29%) korrekt

Tabelle 1: ICMPv6 Testergebnisse

3 Routing Header

Die verschiedenen Arten von Routing Headern (RH) werden in diversen RFCs behandelt.

3.1 RH0

RFC 5095 [**?**] beschreibt die Probleme, die der Routing Header 0 macht und erklärt ihn für veraltet (deprecated). Wenn sein *segments left* Feld 0 ist, soll der Header ignoriert werden und bei einem Wert ungleich 0 mit einem Parameter Problem geantwortet werden.

Basis-Test:
Die ASA verwirft in beiden Fällen das Paket. Dies entspricht einer Fehlerquote von 50% der Testfälle.

3.2 RH2

RFC 3775 [**?**] beschreibt den Mobility Routing Header und legt fest, dass hier das *segments left* Feld den Wert 1 haben muss, um weitergeleitet zu werden.

Basis-Test:
Die ASA verwirft in beiden Fällen (Feld = 1 und Feld $\neq$ 1) das Paket. Dies entspricht einer Fehlerquote von 50% der Testfälle.

3.3 RH200

RFC 2460 [**?**] beschreibt das Verhalten, bei unbekannten Routing Header Typen. Hier entscheidet ebenfalls das *segments left* Feld über das Verhalten. Bei dem Wert 0 wird der Header ignoriert und bei einem Wert ungleich 0 das Paket verworfen (ähnlich wie RH0)

Basis-Test:
Die ASA verwirft in beiden Fällen das Paket. Dies entspricht einer Fehlerquote von 50% der Testfälle.

3.4 Zusammenfassung

Die ASA scheint alle Pakete zu verwerfen, die einen RH beinhalten. Es können explizit RH zugelassen werden, allerdings kann nicht nach dem *segments left* Feld gefiltert werden, was hierfür aber notwendig wäre. Deshalb entfällt hier der Erweiterte-Test. Tabelle 2 fasst die Routing Header Testergebnisse zusammen.

Routing Header	Segments Left	Verhalten	Status
RH0	= 0	Verworfen	inkorrekt
	$\neq 0$	Verworfen	korrekt
RH2	= 1	Verworfen	inkorrekt
	$\neq 1$	Verworfen	korrekt
RH200	= 0	Verworfen	inkorrekt
	$\neq 0$	Verworfen	korrekt

Tabelle 2: Routing Header Testergebnisse

4 IPv6 Header Chain Inspection

RFC 2460 [**?**] spezifiziert das Verhalten für Header Chains.

1. Ein Destination Option (DSTOPT) Header darf höchstens 2 mal auftreten und dann nur vor einem Routing Header und direkt vor dem Upper-Layer Header.
2. Andere Extension Header dürfen nicht mehrfach auftreten.
3. Der Hop-by-Hop (HBH) Header darf nur direkt nach dem IPv6 Base Header erscheinen.

Es wurden folgende Header Profile getestet:

- DSTOPT - muss weitergeleitet werden
- HBH - muss weitergeleitet werden
- DSTOPT,HBH - muss verworfen werden

- DSTOPT,DSTOPT - muss verworfen werden
- HBH,HBH - muss verworfen werden
- DSTOPT,RH,DSTOPT- muss weitergeleitet werden
- HBH,DSTOPT,RH,HBH - muss verworfen werden

Basis-Test:
Die ASA hat die Pakete in 71% der Fälle korrekt behandelt.

Tabelle 3 fasst die ICMPv6 Testergebnisse zusammen.

Header Profil	Verhalten	Status
DSTOPT	Weitergeleitet	korrekt
HBH	Weitergeleitet	korrekt
DSTOPT, HBH	Verworfen	korrekt
DSTOPT, DSTOPT	Weitergeleitet	inkorrekt
HBH, HBH	Verworfen	korrekt
DSTOPT, RH,DSTOPT	Verworfen	inkorrekt
HBH, DSTOPT, RH, HBH	Verworfen	korrekt

Tabelle 3: Header Chain Testergebnisse

Erweiterter-Test:
Eine genaue Filterung nach Reihenfolge oder Anzahl von Vorkommnissen von Headern ist mit der ASA nicht möglich. Man kann jedoch *Inspect Maps* erzeugen. Bei diesen kann man unter anderem *Permit only known extension headers* und *Enforce extension header only* als Option angeben. Ob die Optionen angeschaltet sind oder nicht, hat in den durchgeführten Tests allerdings keine Änderungen bewirkt obwohl die Namen darauf hinweisen würden. Innerhalb solcher *Inspect Maps* kann nach speziellen Headern gefiltert werden. Sind die Filter für die vorkommenden Header aktiviert, funktionieren diese auch und Pakete, die entsprechende Header enthalten werden gefiltert. Das Anschalten einer solchen Inspektion sorgt jedoch schon für ein verbessertes Verhalten (86% korrekt). Tabelle 4 zeigt die Ergebnisse, wenn eine *Inspect Map* definiert ist.

Header Profil	Verhalten	Status
DSTOPT	Weitergeleitet	korrekt
HBH	Weitergeleitet	korrekt
DSTOPT, HBH	Verworfen	korrekt
DSTOPT, DSTOPT	Weitergeleitet	inkorrekt
HBH, HBH	Verworfen	korrekt
DSTOPT, RH,DSTOPT	Weitergeleitet	korrekt
HBH, DSTOPT, RH, HBH	Verworfen	korrekt

Tabelle 4: Header Chain Testergebnisse

5 Overlapping IPv6 Fragments

RFC 5722 [**?**] beschreibt Angriffe auf Basis von fragmentierten Paketen und legt fest, dass Pakete mit Überlappung verworfen werden sollen. Durch Überlappung können wichtige Felder wie z.B. der Port nachträglich verändert werden.

Die folgenden Tests wurden mit fragmentierten Paketen durchgeführt:

- ohne Überlappung (sollte nicht geblockt werden)
- mit Überlappung, die den UDP Port überschreiben soll (sollte geblockt werden)
- mit Überlappung, die den Inhalt des Pakets überschreiben soll (sollte geblockt werden)

Basis-Test:
In allen Fällen reagiert die ASA korrekt auf die Pakete. Dies entspricht einer Fehlerquote von 0% der Testfälle.

Erweiterter-Test:
Kein Erweiterter-Test notwendig.

Tabelle 5 fasst die Ergebnisse des Tests noch einmal zusammen.

Art der Überlappung	Verhalten	Status
Keine	Weitergeleitet	korrekt
UDP Port überschreiben	Verworfen	korrekt
Nutzlast überschreiben	Verworfen	korrekt

Tabelle 5: Overlapping IPv6 Fragments Testergebnisse

6 Tiny IPv6 Fragments

Als Tiny IPv6 Fragements werden Nachrichten bezeichnet, bei denen sich der Upper-Layer Header nicht im ersten Fragment befindet. Hierdurch können in unzureichenden oder fehlerhaften Implementierungen Ports verwendet werden, die eigentlich geblockt werden sollten. Da der Port sich in solch einer Nachricht aber erst in einem späteren Fragment befindet, kann es hier zu Problemen kommen.

Getestet wurden:

- Nachrichten, die im zweiten Fragment einen erlaubten Port beinhalten. Sollte weitergeleitet werden.
- Nachrichten, die im zweiten Fragment einen verbotenen Port beinhalten. Sollte verworfen werden.

Basis-Test:
Die ASA verhält sich in beiden Fällen richtig (0% Fehlerquote).

Erweiterter-Test:
Kein Erweiterter-Test nötig.

Außerdem wird in RFC 2460 [**?**] festgelegt, dass Tiny Fragments nach 60 Sekunden verworfen werden sollen, wenn bis dahin keine weiteren Pakete folgen.

Basis-Test:
Die ASA verwirft Tiny Fragments zu früh und wartet nicht die vorgeschriebenen 60 Sekunden auf andere Fragmente des Pakets.

Erweiterter-Test:
Es ist dem Autor nicht bekannt, dass dieses Timeout in irgendeiner Form manipuliert werden kann. Daher entfällt ein Erweiterter-Test.

Tabelle 6 fasst die Ergebnisse zusammen.

Test	Verhalten	Status
erlaubter Port im 2. Fragment	Weitergeleitet	korrekt
verbotener Port im 2. Fragment	Verworfen	korrekt
Wartet 60 Sekunden	Nein	inkorrekt

Tabelle 6: Behandlung von Tiny IPv6 Fragmenten

7 Excessive Hop-By-Hop Options

In RFC 4942 [**?**] werden verschiedene Sicherheitsaspekte betrachtet. Unter anderem wird beschrieben, dass bis auf Padding Optionen keine Optionen mehrfach im Hop-by-Hop Header auftreten sollen, da dies für Denial-of-Service (DoS) Angriffe genutzt

werden könnte. Gleiche Angriffe könnten auch mit einem Destination Option Header durchgeführt werden, weshalb dieser auch getestet wird.

Es wurden folgende Options Profile für HBH und Destination Option getestet, welche alle verworfen werden sollten:

1. Jumbo Payload, PadN, Jumbo Payload
2. Router Alert, Pad1, Router Alert
3. Quick Start, Tunnel Encapsulation Limit, PadN, Quick Start
4. RPL Option, PadN, RPL Option

Basis-Test:
Die ASA filtert keines der getesteten Pakete. Dies entspricht einer Fehlerquote von 100% der Testfälle.

Erweiterter-Test:
Für diesen Test wurde das IPS Modul aktiviert und zwischengeschaltet. Die vorgenommenen Einstellungen haben allerdings keine Änderung am Ergebnis erzielt (100% Fehlerquote).

Tabelle 7 fasst die Ergebnisse für Hop-By-Hop Options Tests zusammen und Tabelle 8 die für Destination Option Options.

Options Profile	IPS Aktiv	Verhalten	Status
1	Nein	Weitergeleitet	inkorrekt
	Ja	Weitergeleitet	inkorrekt
2	Nein	Weitergeleitet	inkorrekt
	Ja	Weitergeleitet	inkorrekt
3	Nein	Weitergeleitet	inkorrekt
	Ja	Weitergeleitet	inkorrekt
4	Nein	Weitergeleitet	inkorrekt
	Ja	Weitergeleitet	inkorrekt

Tabelle 7: Behandlung von Excessive Hop-By-Hop Options

Options Profile	IPS Aktiv	Verhalten	Status
1	Nein	Weitergeleitet	inkorrekt
	Ja	Weitergeleitet	inkorrekt
2	Nein	Weitergeleitet	inkorrekt
	Ja	Weitergeleitet	inkorrekt
3	Nein	Weitergeleitet	inkorrekt
	Ja	Weitergeleitet	inkorrekt
4	Nein	Weitergeleitet	inkorrekt
	Ja	Weitergeleitet	inkorrekt

Tabelle 8: Behandlung von Excessive Destination Option Options

8 PadN Covert Channel

In RFC 4942 [**?**] wird ebenfalls beschrieben wie die PadN Option verwendet werden kann, um dort Nachrichten illegal zu versenden. PadN wird verwendet, um HBH und DSTOPT Header auf ein vielfaches von 8 Byte zu vergrößern. Dabei dürfen im PadN nur Nullen vorhanden sein. Ein Angreifer kann diese allerdings manipulieren und so als Medium missbrauchen.

Es wurde getestet:

- HBH mit validem PadN
- HBH mit invalidem PadN
- DSTOPT mit validem PadN
- DSTOPT mit invalidem PadN

Basis-Test:
Die ASA hat hier alle Pakete weitergeleitet (50% Fehlerquote der Testfälle) und den Covert Channel somit nicht erkannt und verhindert.

Erweiterter-Test:
Das IPS wurde auf die gleiche Weise wie in Test 7 aktiviert. Das Einschalten des IPS ändert auch hier nichts am Verhalten (50% Fehlerquote).

Tabelle 9 fasst die Ergebnisse für den PadN Covert Channel Test zusammen.

Paket	IPS Aktiv	PadN	Verhalten	Status
HBH	Nein	valide	Weitergeleitet	korrekt
		invalide	Weitergeleitet	inkorrekt
	Ja	valide	Weitergeleitet	korrekt
		invalide	Weitergeleitet	inkorrekt
DSTOPT	Nein	valide	Weitergeleitet	korrekt
		invalide	Weitergeleitet	inkorrekt
	Ja	valide	Weitergeleitet	korrekt
		invalide	Weitergeleitet	inkorrekt

Tabelle 9: PadN Covert Channel Testergebnisse

9 Address Scopes

Mit diesem Test wird überprüft, ob die Firewall sich richtig in Bezug auf den Address Scope verhält. Es wird überprüft, ob Multicast Adressen als Absender akzeptiert werden und ob Link-Local Adressen weitergeleitet werden (beides nicht erlaubt).

Basis-Test:
Die ASA blockiert korrekt alle Pakete, die in dem Test generiert wurden. Dies entspricht einer Fehlerquote von 0% der Testfälle.

Erweiterter-Test:
Ein erweiterter Test ist nicht nötig, da der Basis-Test bereits keine Fehler aufweist.

Tabelle 10 fasst die Ergebnisse für den Address Scopes Test zusammen.

Address Scope	Verhalten	Status
Multicast	Verworfen	korrekt
Link-Local	Verworfen	korrekt

Tabelle 10: Address Scopes Testergebnisse

10 Fazit

Die Protokolltests mit den Default Einstellungen der Cisco ASA 5510 haben gezeigt, dass es häufig zu RFC-unkonformen Verhalten kommt.

Diverse Probleme lassen sich durch das explizite Hinzufügen von Access Rules bzw. Service Policy beheben. Allerdings gilt hier in den meisten Fällen *ganz oder gar nicht*. Eine genauere Filterung wäre hier wünschenswert (Beispielsweise nach *segments left* Feld im Routing Header Beispiel).

Das Anschalten des IPS konnte keine Änderung in den Ergebnissen bewirken. Es kam bei der Konfiguration mit Hilfe des Wizards dazu, dass kein IPv6 Traffic ausgewählt werden konnte. Erst im Nachhinein, wenn die Regel für IPv4 erzeugt wurde, konnte diese noch umgeschrieben werden. Dies führt zur Verwirrung eines ungeübten Nutzers, der evtl. denkt, dass IPv6 nicht unterstützt wird. Hier sollte der Wizard angepasst werden.

Ein weiterer Fehler im ASDM ist aufgefallen, in dem der Befehl bestimmte Pakete zu loggen dazu führt, dass diese Pakete nicht geloggt werden und der Befehl die Pakete nicht zu loggen dazu führt, dass sie geloggt werden (*enable* mit *disable* vertauscht).

Das Testen der bereits erwähnten Service Policies kann für Verwirrung sorgen. Eingetragene Policies werden nämlich erst bei neuen Verbindungen berücksichtigt. Wenn also eine lokale Konfiguration getestet wird, scheint sich z.B. durch das Entfernen einer Policy nichts zu verändern, wenn man diese sofort testet. Man muss erst alle Verbindungen trennen. Dies wiederum geht aber nur über das Kommandozeilen-Tool per *clear conn all* und nicht über einen Button im ASDM. Es gibt allerdings die Möglichkeit direkt Konsolenbefehle über das ASDM an die ASA zu senden. Ohne dieses Wissen kann ein Konfigurationsversuch schnell frustrierend werden.