Best Practices - IMAPS mit TLS

Thomas Fleischmann
Senior Sales Engineer
Central Europe
Thomas.Fleischmann@watchguard.com

WatchGuard Training

Agenda

- Das Protokoll IMAP (mit und ohne S)

- Die Implementierung von IMAP(S) in der Firebox
  - Unverschlüsselter und verschlüsselter Traffic
  - Security Services
  - Reporting / Trouble Shooting

- Live

Das Protokoll IMAP (mit und ohne S)

- Internet Message Access Protocol (IMAP) ist ein Netzwerkprotokoll, das ein Netzwerkdateisystem für E-Mails bereitstellt.

- IMAP wurde in den 1980er Jahren mit dem Aufkommen von Personal Computern entworfen, um bei der Mail-Kommunikation Abhängigkeiten von einzelnen Client-Rechnern aufzulösen.

Das Protokoll IMAP (mit und ohne S)

- Zu diesem Zweck erweitert IMAP die Funktionen und Verfahren von Post Office Protocol (POP) so, dass Benutzer ihre Mails, Ordnerstrukturen und Einstellungen auf den (Mail-)Servern speichern und belassen können. Die (PC-)Clients greifen direkt online auf die Informationen auf den Servern zu und müssen allenfalls Kopien davon beherbergen.
- Während ein Benutzer von POP nach Verlust seines PC entweder alle E-Mails verloren hat oder bereits gelöschte E-Mails erneut erhält, behält ein Benutzer von IMAP seine Mails auf den Servern und, auch über mehrere und verschiedene Clients hinweg, immer einen einheitlichen Zugriff.

Das Protokoll IMAP (mit und ohne S)

- IMAP ist ein textbasiertes Protokoll zum Zugriff auf E-Mails, die sich auf einem Mailserver befinden.

- Ein Mail-Client stellt Anfragen an den Server nur nach aktuell benötigten Informationen. Möchte ein Nutzer z. B. den Inhalt eines Ordners sehen, holt sich der Client eine aktuelle Nachrichtenliste des betreffenden Ordners vom Server. Soll der Inhalt einer Mail angezeigt werden, wird dieser vom Server geladen.

Das Protokoll IMAP (mit und ohne S)

- Da alle Daten weiterhin auf dem Server verbleiben, zeigen – auch bei der Benutzung von mehreren Clients – alle den gleichen, aktuellen Datenbestand einer Mailbox an. Zudem wird eine lokale Speicherung der Daten unnötig und erweiterte Möglichkeiten wie das Durchsuchen von Mails werden serverseitig durchgeführt.

- Um die Daten während der Übertragung vor Dritten zu schützen, kann die Datenverbindung mittels SSL/TLS verschlüsselt werden.

Das Protokoll IMAP (mit und ohne S)

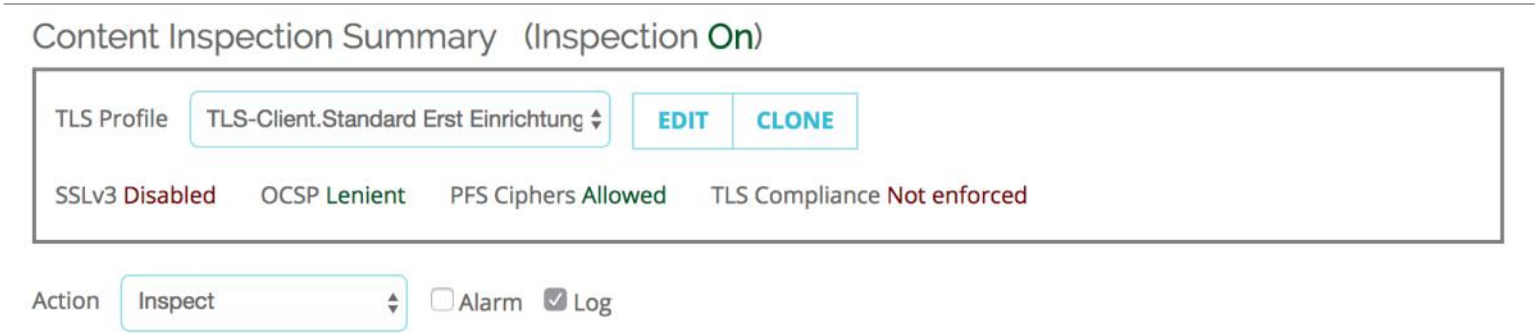
- Bei der Verwendung von IMAPS wird die Verbindung zum Server bereits während des Verbindungsaufbaus durch SSL verschlüsselt. Damit der Server das erkennt, muss ein anderer Port verwendet werden. Dafür wurde der Port 993 reserviert.

- Nach dem Aufbau der SSL-Verbindung wird mindestens IMAPv4 (RFC 3501) verwendet. Die SSL-Schicht ist für das IMAP-Protokoll transparent, d. h., es werden keine Änderungen am IMAP-Protokoll vorgenommen.

Die Implementierung von IMAP(S) in der Firebox

- Die Absicherung von IMAP(S) wird mit einen eigenen Proxy in der Firebox umgesetzt.
- Dieser Proxy besteht aus denselben Elementen, wie andere Proxy Konfigurationen.

- Neu hinzugefügt wurde die Einstellung zum Bereich TLS.
  - Um TLS aktiv nutzen zu können, muss Content Inspection in den Proxy Action unter den Bereich TLS ausgewählt sein.

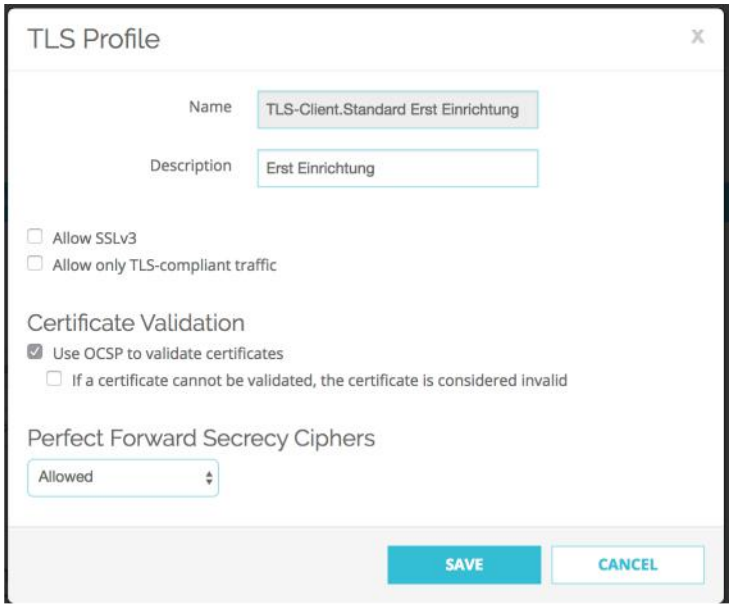


Die Implementierung von IMAP(S) in der Firebox

- Im TLS Profil kann man folgende Parameter einstellen:

- *Allow SSLv3*
- *Allow only TLS-compliant traffic*
- *Use OCSP to validate certificates*

- *Perfect Forward Secrecy Ciphers*
  - **None**
  - **Allowed**
  - **Required**



Die Implementierung von IMAP(S) in der Firebox

- Mit der Einführung des TLS Profil hat sich nicht nur beim IMAP(S) Proxy was geändert, sondern auch im Bereich HTTP(S) Proxy.
- Auf der Firebox wurden vordefinierte TSL Profile angelegt

TLS Profile	OCSP	TLS Compliance	Used By Proxy Actions
TLS-Client.Standard	Disabled	Not enforced	IMAP-Client.Standard
TLS-Server.Standard	N/A	Enforced	IMAP-Server.Standard
TLS-Client-HTTPS.Standard	Lenient	Not enforced	HTTPS-Client.Standard HTTPS-Client
TLS-Server-HTTPS.Standard	N/A	Not enforced	HTTPS-Server.Standard HTTPS-Server

- Es ist möglich, diese Profile zu klonen und entsprechend im Proxy unter TLS Profile angepasst zu verwenden.

Die Implementierung von IMAP(S) in der Firebox

- Bei der Erstellung eines IMAP(S) Proxy, kann man das Verhalten des IMAP(S) Proxy definieren unter den Bereich „Settings“.

- Disabled - IMAP Proxy horcht nur auf Port 143
- Enabled - IMAP Proxy horcht auf Port 143 und 993 (Default)
- Required - IMAP Proxy horcht nur auf Port 993

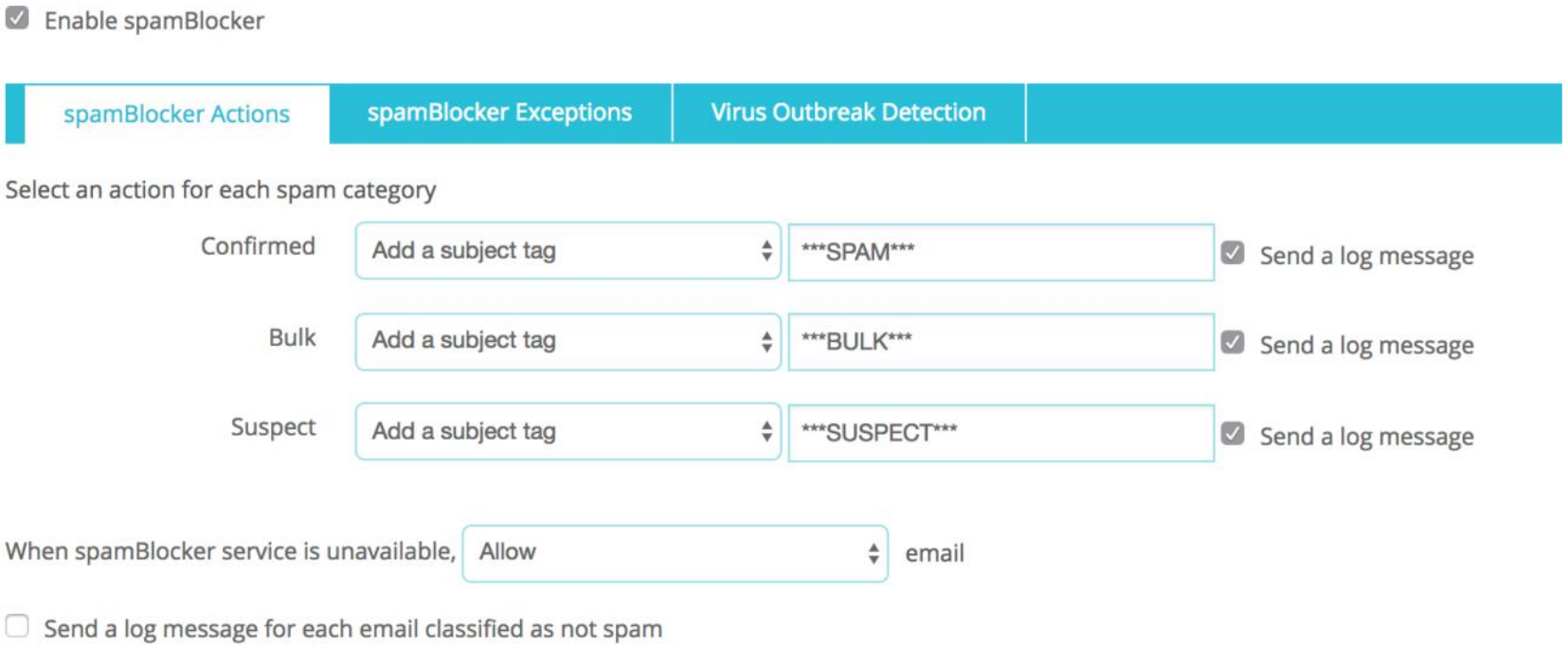
Die Implementierung von IMAP(S) in der Firebox

- Im Bereich der Konfigurationen der Proxy Actions sind folgende Anmerkungen zu beachten.

a) Im Bereich „Attachments“ unter „Content Types“ immer den Punkt „Enable content type auto detection“ aktivieren.

Die Implementierung von IMAP(S) in der Firebox

b) Der SpamBlocker erlaubt das Taggen einer Email. Weitere Funktionen wie bei SMTP oder POP3 sind nicht gegeben, weil das IMAP Protokoll dies nicht ermöglicht.



Die Implementierung von IMAP(S) in der Firebox

- Eine wichtige Neuerung existiert seit kurzen beim APT Blocker!!
  - Der IMAP Proxy untersucht alle Datei Anhänge in der Email.
  - Die Email wird erst zugestellt, wenn alle Anhänge analysiert sind und ein eindeutiges Ergebnis vorliegt.
  - Wenn der Timeout vor der Analyse eintritt, wird beim nächsten Abruf der Dateien das nun vorliegende Ergebnis verwendet und die Email mit oder ohne Anhang zugestellt.

Die Implementierung von IMAP(S) in der Firebox

- Man kann im Diagnostic Log oder im IMAP Proxy selber das Log Level anpassen, um weitere Informationen zum Datenverkehr zu erlangen.

- Aus - Für diese Kategorie werden keine Diagnoseprotokollmeldungen gesendet.
- Fehler - (Standardeinstellung) Diese Stufe enthält Protokollmeldungen für schwerwiegende Fehler.
- Warnung - Diese Ebene enthält Details zu abnormalen Zuständen, die dazu beitragen, Verhaltensprobleme zu erklären, sowie Informationen zur Fehlerstufe.
- Information - Diese Ebene enthält Details zum erfolgreichen Betrieb, sowie Informationen aus den Fehler- und Warnstufen.
- Debug - Diese Ebene enthält detaillierte Protokollmeldungen für alle Protokollebenen.

Die Implementierung von IMAP(S) in der Firebox

- Unter Dimension werden die Logs zum IMAP ausgewertet.

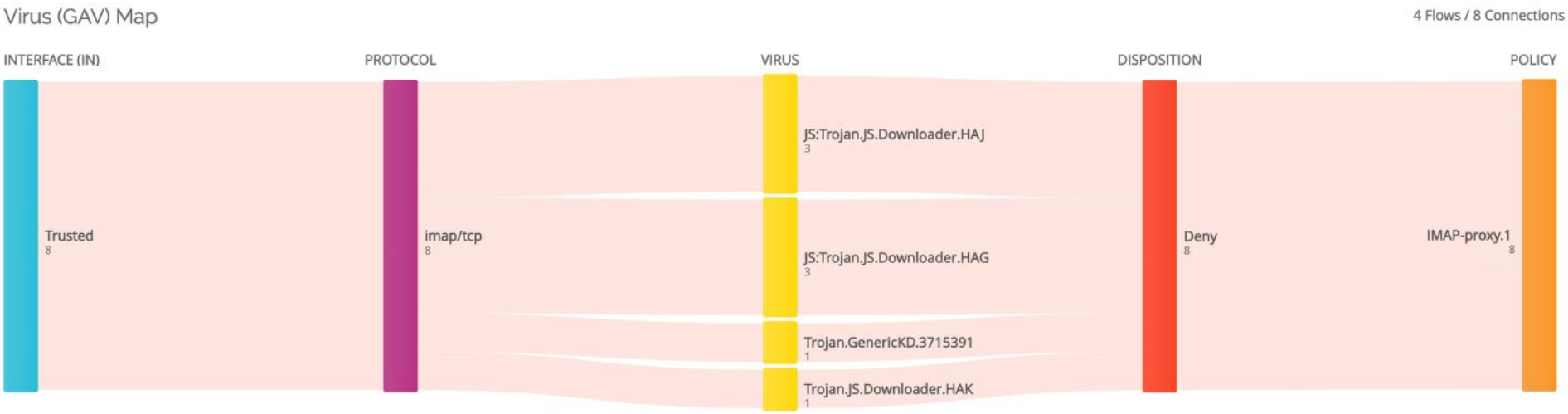
Home / Hetzner_Firebox_01 / Virus (GAV) / imap/tcp

Virus (GAV) Protocol: imap/tcp

Page 1 of 1 100

DISPOSITION	TIME	VIRUS	SOURCE	DESTINATION	POLICY	PROTOCOL	HOST	SENDER	RECIPIENTS	HITS
Stripped	2018-04-20 11:02:33	Trojan.GenericKD.371!	10.0.1.12	85.13.140.190:143	IMAP-proxy.1-00	imap/tcp				1
Stripped	2018-04-20 11:02:35	Trojan.JS.Downloader.	10.0.1.12	85.13.140.190:143	IMAP-proxy.1-00	imap/tcp				1
Stripped	2018-04-20 11:02:36	JS:Trojan.JS.Downloa	10.0.1.12	85.13.140.190:143	IMAP-proxy.1-00	imap/tcp				3
Stripped	2018-04-20 11:02:36	JS:Trojan.JS.Downloa	10.0.1.12	85.13.140.190:143	IMAP-proxy.1-00	imap/tcp				3

Page 1 of 1 100



Live Demo

Vielen Dank!

WatchGuard Training

NOTHING GETS PAST RED.

WatchGuard Training