agree21Internet

Atruvia Secure Webgateway

ATRUVIA

Genossenschaftliche FinanzGruppe
Volksbanken Raiffeisenbanken

agree21Internet - Atruvia Secure Webgateway

Inhaltsverzeichnis

Vorbemerkung: Technische Daten zur Konfiguration

Die Konfiguration der Endgeräte erfolgt in der Regel automatisch über Windows Gruppenrichtlinienobjekte (GPO). Über diese werden die sogenannte Proxyautokonfiguration (PAC) und gegebenenfalls auch die von der Windows Command Line (CMD) verwendete statische Proxykonfiguration an die Endsysteme verteilt.

Statische Proxykonfiguration

Sollte es einmal notwendig sein, in einem Softwareprodukt oder einem speziellen Endgerät die Proxykonfiguration manuell vorzunehmen, verwenden Sie bitte folgende Angaben:

Proxyautokonfiguration (PAC-Datei): http://kunden-proxypac.rz.bankenit.de/

Proxyadresse: kunden-proxy.rz.bankenit.de:8080

Ausgehende öffentliche Adressen der Atruvia Secure Webgateways

Sollten Sie mit einem Drittanbieter zusammenarbeiten, der die Zugriffe auf seine Systeme auf Netzwerkebene einschränkt, teilen Sie diesem für die Firewallkonfiguration bitte folgende Netze mit:

- 194.149.246.0/24
- 195.200.34.0/24
- 195.200.47.0/24

1 Funktionsbeschreibung agree21Internet - Atruvia Secure Webgateway

Das Atruvia Secure Webgateway ist Teil des Produkts agree21Internet und basiert technisch auf dem Produkt „Skyhigh Secure Web Gateway“ der Firma Skyhigh. Es dient dazu, anhand von definierten Kriterien bestimmte Websites zu blockieren bzw. explizit freizugeben und somit einen sicheren Internetzugangs für den Nutzer bereitzustellen. Dabei werden Techniken wie URL-Kategorisierung, Whitelisting, Media Type Filter, Virus Scanning und SSL-Analyse eingesetzt.

Das Atruvia Secure Webgateway ist seitens Atruvia bereits optimal vorkonfiguriert und erlauben Ihnen den sicheren Zugriff auf das Internet. Darüber hinaus erlaubt es Ihnen, die Zugriffsberechtigungen auf das Internet individuell auf Ihre Bedürfnisse anzupassen.

Alle Internetzugriffe über das Netz der Atruvia durchlaufen das Atruvia Secure Webgateway. Hierzu zählen auch Zugriffe von mobilen Arbeitsplätzen, sofern diese über das VPN der Atruvia eingewählt sind.

1.1 Allgemein

Atruvia bietet Ihnen mit dem Produkt unter anderem:

- Drei vorkonfigurierte, unterschiedlich abgestufte Profile, die entweder sofort verwendbar sind oder als Ausgangspunkt für individuell konfigurierte Profile verwendet werden können.

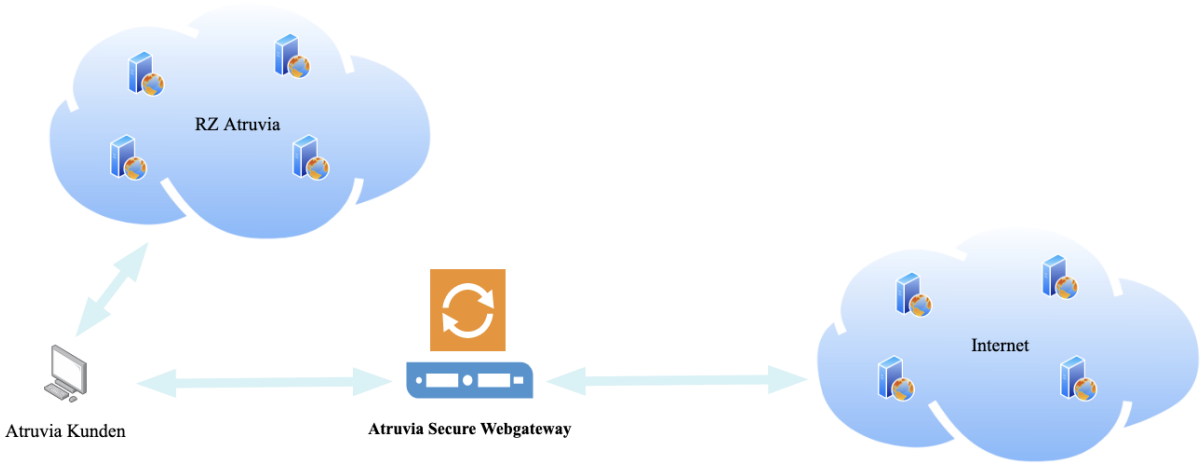
- Das Atruvia Secure Webgateway bietet Ihnen bis zu zwanzig unterschiedliche Profile, wobei siebzehn davon individuell konfigurierbar sind.

- Sie können verschlüsselte Kommunikationsbeziehungen entschlüsseln und über das Atruvia Secure Webgateway analysieren. Dadurch erkennen Sie potenziell gefährliche Inhalte und können diese sperren.

- Viele Einstellungen, die zuvor nur durch einen Atruvia-Mitarbeiter vorgenommen werden konnten, lassen sich nun von Ihnen durchführen. Dies erleichtert Ihnen die Administration und bietet mehr Flexibilität.

2 Atruvia Secure Webgateway - was genau ist das eigentlich?

Für alle technisch Interessierten bietet dieses Kapitel nützliche Informationen und beantwortet viele Fragen bezüglich der technischen Realisierung des Atruvia Secure Webgateways.



2.1 Der Proxy

2.1.1 Funktionsweise des Proxys

Anders als bei den meisten Internetanschlüssen zu Hause verbindet sich ein Computer, der über das Atruvia Secure Webgateway auf das Internet zugreift, nicht direkt mit dem Zielsystem. Der Zugriff geschieht über einen Proxy (wörtlich: Stellvertreter). Auf diese Weise kann ein potenziell bösartiges Zielsystem nicht direkt mit dem anfragenden Computer kommunizieren. Der direkte Zugriff wird durch den Proxy technisch verhindert.

2.1.2 Besonderheiten des Atruvia Secure Webgateway

Der Vorteil des Atruvia Secure Webgateway liegt in den erweiterten Proxy-Funktionalitäten. Das System bietet unter anderem die Möglichkeit, übertragene Daten auf Malware zu prüfen und Zieladressen anhand von Filterlisten und Kategorisierungen gezielt zu sperren oder freizugeben. Weitere Details zum Thema Proxy finden Sie unter anderem hier:
https://de.wikipedia.org/wiki/Proxy_(Rechnernetz)

2.2 Der Filter

Die Atruvia Secure Webgateways (siehe schematische Darstellung in Kapitel 2) sind Proxy-Server. Diese sind zu einer Kette (Proxy-Chain) in Reihe geschaltet. Das Atruvia Secure Webgateway (orange) bietet die Möglichkeit, Inhalte innerhalb der Internetverbindung zu „filtern“.

2.2.1 Interpretation der Kommunikation

Damit das Atruvia Secure Webgateway als Stellvertreter für den anfragenden Computer (Atruvia-Kunden) agieren kann, muss dieser das verwendete Netzwerkprotokoll verstehen. Das Atruvia Secure Webgateway interpretiert den Inhalt der Kommunikation und gibt die Informationen intern an diverse Sicherheitsmodule weiter, bevor diese endgültig an das Zielgerät/Internet gelangen

(dies gilt ebenso für den Rückweg – Inhalt vom Internet zum Computer). Diese Module sind auf jeweils eine bestimmte Aufgabe spezialisiert.

- Die Prüfung auf Viren.
- Das Aufbrechen von verschlüsselten Verbindungen damit diese auch auf Viren geprüft werden können.
- Das Sperren bestimmter Inhalt (z. B. pornografische Inhalte).
- Das Sperren bestimmte Dateitypen (z. B. .exe-Dateien).

2.2.2 Weitere Kommunikationsbeziehungen im Internet

Websites werden für gewöhnlich über das Internetprotokoll http (TCP-Port 80) oder https (TCP-Port 443) übertragen.

Das Internet besteht jedoch nicht nur aus Websites. Es gibt eine Vielzahl anderer Kommunikationsbeziehungen wie z. B. Internettelefonie, Remoteadministration, Peer-to-Peer. Das Atruvia Secure Webgateway unterstützt viele dieser Internetprotokolle und überprüft deren Kommunikation.

Bitte beachten Sie, dass es sich beim Atruvia Secure Webgateway um einen TCP-Proxy handelt und daher UDP-Verbindungen systembedingt nicht unterstützt werden.

3 Secure Webgateway Funktionen im Detail

3.1 Filter-Möglichkeiten

3.1.1 URL-Filter

Der URL-Filter ermöglicht das Sperren bestimmter Zieladressen im Internet. So lassen sich auf Basis einer Internetdomäne oder einer exakten/vollständigen URL-Inhalte sperren bzw. freigeben.

3.1.2 Kategorie-Filter

Der Kategorie-Filter ermöglicht das Sperren einzelner Kategorien z. B.: Webmailer, Drogen etc.

3.1.3 Webinhalte-Filter

Der Webinhalte-Filter erlaubt das Sperren von Inhalten aufgrund des Medientyps. So können beispielsweise ausführbare Dateien wie EXE-Dateien oder Videos wie MP4-Dateien anhand des sogenannten Mime-Types gesperrt werden.

3.1.4 Malware-/Virusfilter

Der Malware-/Virusfilter prüft unabhängig von der aufgerufenen Website jeglichen übertragenen Inhalt auf Schadsoftware. Dieser Filter ist standardmäßig aktiviert und benötigt keinerlei weitere Konfiguration. Sollte ein Virus gefunden werden, so wird die Datei, die den Virus enthält, zurückgehalten und nicht zum Computer übertragen. Wird für den Internetzugriff ein Browser verwendet, erscheint eine entsprechende Information für den Benutzer.

Wird der Malware-/Virusfilter mit aktivierter SSL-Analyse (standardmäßig nur im Managed Stufe 1-3 aktiviert) verwendet, so werden auch Dateien, die über eine verschlüsselte Verbindung übertragen werden, auf Schadsoftware geprüft. Ist die SSL-Analyse deaktiviert, ist eine Prüfung auf Schadsoftware innerhalb einer verschlüsselten Verbindung technisch nicht möglich. Ein Virus wird in diesem Fall in der Regel von den lokal installierten Viren/Malwareschutz auf dem Computer des Benutzers erkannt und unschädlich gemacht.

3.2 SSL-Analyse

Achtung: Dieser Abschnitt enthält wichtige Informationen, die sie unbedingt vor der Aktivierung der SSL-Analyse lesen sollten.

3.2.1 Funktionsweise

SSL (https://de.wikipedia.org/wiki/Transport_Layer_Security) ist eine Technik zum Verschlüsseln von Inhalten. Verschlüsselte Daten können weder mitgelesen noch verändert werden. Aus diesem Grund können verschlüsselte Daten grundsätzlich nicht auf schädlichen Inhalt geprüft werden.

Die SSL-Analyse ermöglicht es, verschlüsselte Verbindungen auf dem Atruvia Secure Webgateway zu entschlüsseln und zu interpretieren. Der Datenstrom wird dazu zuerst vom Atruvia Secure Webgateway entschlüsselt, anschließend auf Schadsoftware überprüft und danach wieder verschlüsselt.

3.2.2 Empfehlung zur Aktivierung

Atruvia empfiehlt grundsätzlich die Aktivierung der SSL-Analyse. Die von Atruvia betreuten und konfigurierten Internetbrowser sind immer bereits für die Verwendung der SSL-Analyse vorbereitet.

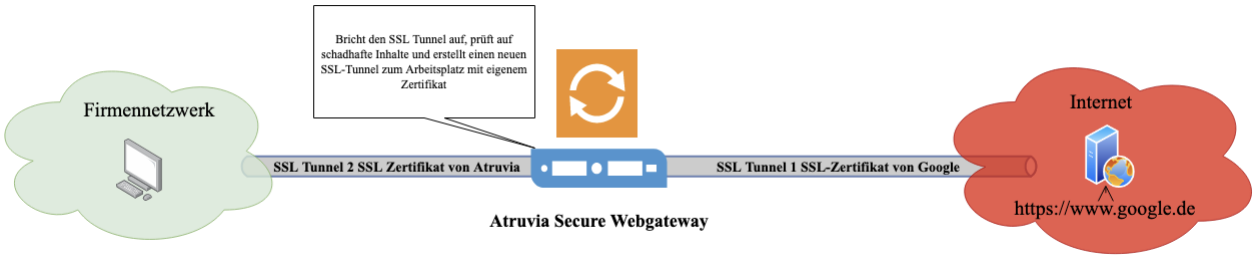
Da sich jedoch durch die SSL-Analyse möglicherweise Änderungen im Verhalten einzelner Softwareprodukte ergeben können, planen und verproben Sie die Aktivierung bitte unbedingt auf einem einzelnen Internetprofil.

Die SSL-Analyse ist abgesehen von den Profilen Managed Stufe1-3 standardmäßig deaktiviert.

3.2.3 Verbindungen ohne und mit SSL-Analyse

Ohne SSL-Analyse – Der SSL-Tunnel wird nicht unterbrochen. Die Verbindung ist vom Arbeitsplatz bis zum Webserver mit dem Zertifikat des Websitebetreibers verschlüsselt, nicht lesbar und somit nicht auf Viren/Malware prüfbar.

Mit SSL-Analyse – Der SSL-Tunnel wird aufgebrochen. Die Verbindung ist vom Atruvia Secure Web Gateway bis zum Webserver mit dem Zertifikat des Websitebetreibers verschlüsselt.
Vom Atruvia Secure Webgateway zum Arbeitsplatz wird ein separater SSL-Tunnel aufgebaut, der mit dem Zertifikat der Atruvia verschlüsselt ist.



3.2.4 Erneute Verschlüsselung

Damit am Endgerät (i.d.R. dem Browser) verschlüsselte Daten ankommen, muss die SSL-Analyse die Verschlüsselung nach der Prüfung wieder rückgängig machen. Da die SSL-Analyse jedoch nicht im Besitz der hierfür notwendigen Datenschlüssel ist (diese hat nur der Urheber - i.d.R. der Webmaster der angefragten Website) kann dies nicht geschehen. Stattdessen werden die Daten mit einem eigenen Datenschlüssel erneut verschlüsselt. Dieser wird im Browser anstelle des originalen Schlüssels angezeigt:

Dieses Verhalten entspricht einem sogenannten Man-In-The-Middle, bekannt durch die sogenannte Man-In-The-Middle Attacke. Hier wird diese jedoch nicht als Angriff, sondern als Sicherheitslösung angewendet.

Der Original-Datenschlüssel der angefragten Website ist nicht sichtbar. Im Browser wird lediglich das Zertifikat von Atruvia angezeigt. Die Überprüfung auf Korrektheit und Gültigkeit wird nicht, wie bisher, am Browser durch den Benutzer bzw. der dort hinterlegten Prüfstellen ausgeführt, sondern automatisiert am zentralen Atruvia Secure Webgateway anhand von installierten und regelmäßig aktualisierten Prüfstellen.

Um den Original-Datenschlüssel angezeigt zu bekommen, muss die Ziel-URL über die entsprechende Whitelist von der SSL-Analyse ausgenommen werden. Dann kann jedoch die Verbindung nicht mehr auf Malware geprüft werden.
Eine erweiterte Prüfung des Schlüssels bietet der Dienst https://www.ssllabs.com/ssltest/ an.

3.2.5 SSL-Analyse Besonderheiten

Bei deaktivierter SSL-Analyse werden verschlüsselte Daten (https) am Atruvia Secure Webgateway lediglich durchgeleitet. Technisch bedingt könne verschlüsselte Verbindungen (https) dann nicht am Atruvia Secure Webgateways überprüft werden. Daraus ergeben sich folgende Einschränkungen:

- Kein Malwarescan möglich
- URL-Filter: Keine Prüfung auf den URL-Pfad möglich. Konfigurationseinträge, welche einen URL-Pfad enthalten, greifen nicht. (Einträge, welche keinen URL-Pfad enthalten, funktionieren auch ohne aktives SSL-Scanning.)
- Sperre von verschlüsselten Websockets nicht möglich.
- Medientypfilter greift nicht.

Unverschlüsselte Verbindungen (http) sind von diesen Ausnahmen nicht betroffen.
Kategorie-Filter, Reputation, URL-Filter ohne URL-Pfad funktionieren auch ohne aktives SSL-Scanning.

Bei aktivierter SSL-Analyse ist auch bei verschlüsselten Verbindungen (https) der volle Funktionsumfang gegeben.

4 Bedienungsanleitung/Handhabung Secure Webgateway

4.1 Administrationsoberfläche

Die Administration erfolgt vollumfänglich in SAGA.

4.1.1 Zugriffsberechtigung

Als Administrator benötigen sie keine separate Berechtigung zur Administration.

4.1.2 Erfolgreiche Anmeldung

Nach erfolgreicher Anmeldung navigieren sie zum Menüpunkt
Infrastruktur ➔ Netz ➔ agree21Internet

4.2 Das Listen-Prinzip

Die Konfiguration des Secure Webgateways basiert auf einem Regelwerk mit Regeln und Listen.

Um den Prozess für Sie so einfach und transparent wie möglich zu gestalten, haben wir uns entschieden sogenannte Smartlisten einzuführen. Smartlisten werden verwendet, wenn Sie Host, Domain oder URLs für Ausnahmen oder Freischaltungen konfigurieren.

SmartList-Einträge können sowohl aus Hostnamen, als auch aus Domains, URLs oder auch Fragmenten einer URL bestehen. Wichtig ist hier, dass keine Wildcards verwendet werden dürfen. Das Platzhalterzeichen * ist nicht erlaubt.

Beispieleinträge:

Eintrag in der Liste	Entspricht der Einstellung
meinesubdomain.atruvia.de	*.meinesubdomain.atruvia.de meinesubdomain.atruvia.de
http://atruvia.de	http://*.atruvia.de http://atruvia.de
atruvia.de/sitemap	*.atruvia.de/sitemap* atruvia.de/sitemap*
/sitemap	*/sitemap* (Sollte so nicht verwendet werden und ist nur der Vollständigkeit halber hier aufgeführt)

Beispiele für geeignete Einträge:

Eintrag: atruvia.de
Mit diesem Eintrag würden alle Subdomänen von atruvia.de korrekt übereinstimmen, einschließlich atruvia.de, www.atruvia.de, secure.atruvia.de usw.

Eintrag: https://atruvia.de
Wie oben, allerdings eingeschränkt auf HTTPS-Verbindungen.

Eintrag: atruvia.de/meineseite/sitemap/
Mit diesem Eintrag stimmen alle Inhalte der Domäne "atruvia.de" überein, die den Pfad "/meineseite/sitemap/" enthalten.

Beispiele für Einträge, wie man sie nicht verwenden sollte:

Eintrag: /meineseite/sitemap/
Die Verwendung dieses Eintrags könnte möglicherweise zu Übereinstimmungen mit anderen Hosts führen, die den Pfad "/meineseite/sitemap/" enthalten,
z. B.: http://eineboeseseite.com/meineseite/sitemap/

Eintrag: *.atruvia.de
Wildcards werden in URL.SmartMatch-Einträgen nicht verwendet.

Eintrag: *.atruvia.de/*
Wildcards werden in URL.SmartMatch-Einträgen nicht verwendet.

Eintrag: .atruvia.de
Ein führender Punkt führt dazu, dass der Eintrag nicht übereinstimmt.

Einträge, die auf den Pfad eines Aufrufs filtern, wie beispielsweise
https://www.atruvia.de/meineseite/sitemap/
funktionieren nur bei aktivierter SSL-Analyse. Ohne SSL-Analyse ist es technisch nur möglich den Host, auf den der Connect stattfindet, zu sehen.
Ebenfalls nicht auf den URL-Pfad geprüft werden kann für URLs in den Menüpunkten „Sperren“, „Freischaltungen“, Authentifizierungsausnahmen und SSL>>Ausnahmen. Sollen einzelne URLs mit Angabe des URL-Pfades gesperrt werden, so muss SSL-Scanning aktiv sein und die Sperre unter Ziel sperren>>Adresse hinterlegt werden.

Beispiel:

Mit SSL-Analyse sieht der Proxy den Aufruf:
https://www.atruvia.de/meineseite/sitemap/

Ohne SSL-Analyse sieht der Proxy den Aufruf:
www.atruvia.de

4.3 Anzahl der Internetprofile

Ihnen stehen drei Internetprofile mit Vorgaben und Einstellungen durch die Atruvia zur Verfügung. Die drei vorgebebenen Profile können inhaltlich nicht modifiziert werden. Die Einstellungen zu diesen Profilen werden später in diesem Kapitel noch erläutert.

Zusätzlich stehen ihnen 17 weitere Internetprofile für individuelle Konfigurationen zur Verfügung, um beispielsweise unterschiedliche Abteilungen mit unterschiedlichen Internetzugriffsberechtigungen abzubilden.

Zusätzlich zu den 20 Profilen stehen ihnen noch jeweils eine globale Whitelist und Blacklist zur Verfügung, mit denen sie für ihr Institut (unabhängig von der Benutzerzuordnung) Freischaltungen durchführen können.

4.4 Klonen von Internetprofilen

Sie können ein bereits vorhandenes Profil jederzeit als Ausgangspunkt für die Anlage eines neuen Profils verwenden. Wählen Sie dazu bei der Anlage aus dem Dropdown-Menü "Kopie von:" das zu

verwendende Profil aus. Sämtliche Einstellungen des Ausgangsprofils werden für das neu angelegte Profil übernommen und können danach beliebig angepasst werden.

4.5 Darstellung der Einstellungen für die Profile Managed Stufe 1-3

4.5.1 Managed Stufe 1

Gesperrte Kategorien:

Kategorien	Unterkategorie
Risk / Fraud / Crime	Malicious Downloads
	Illegal UK
	Browser Exploits
	Phishing
	Spyware / Adware / Keyloggers
	Malicious Sites
	Anonymizing Utilities
	Anonymizers

Unkategorisierte Seiten: Nicht gesperrt
Gesperrte Reputation: Hohes Risiko (Websites mit hohem Risiko werden gesperrt)
SSL-Analyse: Aktiviert (Netzwerkverkehr wird zur Analyse entschlüsselt)
Websockets sperren: Aktiviert (Websockets sind nicht erlaubt)

4.5.2 Managed Stufe 2

Gesperrte Kategorien:

Kategorien	Unterkategorie
Risk / Fraud / Crime	Malicious Downloads
	Illegal UK
	Browser Exploits
	Consumer Protection
	Residential IP Addresses
	Phishing
	Spyware / Adware / Keyloggers
	P2P / File Sharing
	Malicious Sites
	Parked Domains
	Potential Hacking / Computer Crime
	Anonymizing Utilities
	Anonymizers
Pornography / Nudity	Pornography
	Nudity
Mature / Violent	Extreme
Information Technology	Personal Network Storage
	Remote Access
Information / Communication	WebMail
Drugs	Drugs

Unkategorisierte Seiten: Nicht gesperrt
Gesperrte Reputation: Hohes Risiko (Websites mit hohem Risiko werden gesperrt)
Gesperrte Medientypen: application/executable (Ausführbare Dateien .exe, werden gesperrt)
SSL-Analyse: Aktiviert (Netzwerkverkehr wird zur Analyse entschlüsselt)
Websockets sperren: Aktiviert (Websockets sind nicht erlaubt)

4.5.3 Managed Stufe 3

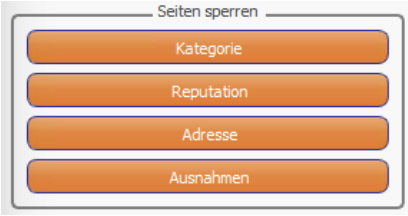
Gesperrte Kategorien:

Kategorien	Unterkategorie
Society / Education / Religion	For Kids
	Major Global Religions
	Religion / Ideology
	Politics /Opinion
	Non-Profit / Advocacy / NGO
	Government / Military
Risk / Fraud Crime	PUPs
	Malicious Downloads
	Illegal UK
	Consumer Protection
	Browser Exploits
	Residential IP Addresses
	Historical Revisionism
	Parked Domain
	Potential Illegal Software
	Spam URLs
	Phishing
	School Cheating Info
	Spyware / Adware / Keyloggers
	P2P / File Sharing
	Malicious Sites
	Discrimination
	Potential Hacking / Computer Crime
	Potential Criminal Activities
	Anonymizing Utilities
	Anonymizers
Purchasing	Auctions / Classifieds
	Fashion / Beauty
	Marketing / Merchandising
	Motor Vehicles
	Online Shopping
	Pharmacy
Pornography / Nudity	Incidential Nudity
	Sexual Materials
	Pornography
	Provocative Attire
	Nudity
Mature / Violent	Game /Cartoon Violence
	Gruesome Content
	Profanity
	Weapons
	Violence
	Extreme
Lifestyle	Controversial Opinions
	Social Networking
	Dating / Personals
	Restaurants
	Travel
	Sports
	Personal Pages
Information Technology	Personal Network Storage
	Webads
	Shareware / Freeware
	Resource Sharing
	Remote Access
Information / Communication	Portal Sites
	Digital Postcards
	Messaging
	Forum / Bulletin Boards
	Web Phone
	Web Mail
	Portal Sites
	Mobile Phone
	Instant Messaging
	Chat

Games / Gambling	Gambling Related
	Games
	Gambling
Entertainment / Culture	Recreation / Hobbies
	Media Sharing
	Streaming Media
	Media Downloads
	Internet Radio / TV
	Humor / Comics
	Entertainment
	Art / Culture / Heritage
Drugs	Tobacco
	Drugs
	Alcohol
Business / Services	Job Search

Unkategorisierte Seiten: Gesperrt
Gesperrte Reputation: Mittleres/Hohes Risiko (Websites mit hohem oder mittlerem Risiko werden gesperrt)
Gesperrte Medientypen: application/executable (Ausführbare Dateien .exe, werden gesperrt)
SSL-Analyse: Aktiviert (Netzwerkverkehr wird zur Analyse entschlüsselt)
Websockets sperren: Aktiviert (Websockets sind nicht erlaubt)

4.6 Seiten sperren



4.6.1 Kategorien

Hier können sie die gewünschten Kategorien oder Unterkategorien für das ausgewählte Internetprofil sperren.

Mit dem Kategorie-Filter stehen Ihnen eine Vielzahl an Kategorien (wie z. B. Shopping, Social Networks, Phishing, Anonymizers, Violence, Webmail, Gambling) zur Verfügung. Wird eine der Kategorien ausgewählt, so werden alle Websites, die in dieser Kategorie enthalten sind, gesperrt. Die Zuweisung von Websites zu einer Kategorie findet größtenteils automatisiert durch einen Dienstleister statt.

Eine Website kann aufgrund des Inhaltes auch zu mehreren Kategorien gehören. In diesem Fall wird die Website bereits gesperrt, sobald eine der für die Website zutreffenden Kategorien als Sperre eingetragen wurde.

Ausnahmen lassen sich über die Schaltfläche „Ausnahmen“ definieren.

Eine Neu- bzw. Umkategorisierung einer Website können Sie beim Dienstleister über die folgende Adresse beauftragen:

https://trustedsource.org/
(Skyhigh Secure Web Gateway Appliances (SWG for On-Prem) – with GTI Lookup)

An dieser Webseite sollten Sie sich sich zuvor anmelden, da nur dann eine Ein- bzw. Umkategorisierung mit hoher Priorität durchgeführt wird. Die Registrierung ist kostenlos.

In der Standardeinstellung erlaubt das Atruvia Secure Webgateway den Zugriff auf nicht kategorisierte (uncategorized) Websites. Dieses Verhalten kann geändert werden, indem sie in SAGA das gewünschte Internetprofil auswählen und unter Kategorie den Haken „unkategorisierte Webseiten sperren“ setzen.

Achtung: Das Secure Webgateway führt auf aktuell nicht kategorisierte Websites eine lokale Analyse durch. Dies kann dazu führen, dass Websites, die aktuell nicht kategorisiert sind, trotzdem einer Kategorie zugewiesen werden und somit erlaubt werden, falls die gefundene Kategorie nicht in der Kategorieliste gesperrt wurde. Solche Websites werden automatisch zur exakten Analyse an TrustedSource gesendet und können dann in einigen Tagen dort entsprechend abgefragt werden.

Eine Übersicht der verfügbaren Kategorien, inkl. Beschreibung, kann direkt vom Hersteller bezogen werden https://trustedsource.org/
Direktlink https://www.trustedsource.org/download/ts_wd_reference_guide.pdf

4.6.2 Reputation

Jede URL hat neben einer Kategoriezuweisung auch eine Reputation: Low, Medium oder High Risk. Die Zuordnung findet automatisiert statt. Als High Risk werden in der Regel nur Websites eingestuft, die aktuell oder kürzlich mit Malware infiziert waren. Alle übrigen Websites sind für gewöhnlich als Low Risk oder Medium Risk eingestuft.

Sie können hier definieren, ob die Reputationsprüfung genutzt werden soll. Aktivieren Sie hierzu eine der beiden Optionen "Mittleres/Hohes Risiko" oder "Hohes Risiko".

Ausnahmen lassen sich über die Schaltfläche „Ausnahmen“ definieren.

Auch die URL-Reputation kann über den Dienstleister zur Neubewertung gegeben werden:

https://trustedsource.org/
(Skyhigh Secure Web Gateway Appliances (SWG for On-Prem) – with GTI Lookup)

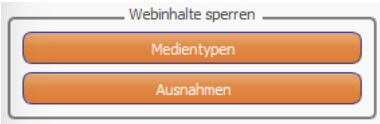
4.6.3 Adresse

Hier können sie gezielt Adressen oder Ziele für den Zugriff sperren.
Beispiele für die Verwendung finden sie im Kapitel 4.2 Das Listen-Prinzip.

4.6.4 Ausnahmen

Hier können sie gezielt Adressen oder Ziele für den Zugriff freigeben
Beispiele für die Verwendung finden sie im Kapitel 4.2 Das Listen-Prinzip.

4.7 Webinhalte sperren



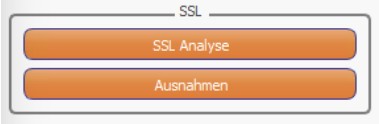
4.7.1 Medientypen

Hier können sie gezielt Medientypen wie EXE oder ZIP-Dateien anhand des Mime-Types sperren.

4.7.2 Ausnahmen

Hier können sie gezielt Adressen oder Ziele angeben, die trotz einer gesetzten Webinhalt-Sperre im Internetprofil erlaubt sein sollen.
Beispiele für die Verwendung finden sie im Kapitel 4.2 Das Listen-Prinzip

4.8 SSL



4.8.1 Information Ihrer Mitarbeiter

Bitte informieren Sie ihre Anwender, wenn Sie die SSL-Analyse aktivieren und informieren Sie diese, dass der Datenschlüssel vom Proxy ausgetauscht wird, da es sonst leicht zu Missverständnissen bezüglich der Sicherheit der Datenverbindung ins Internet kommen kann.

4.8.2 Mögliche Gründe für eine Ausnahme von der SSL-Analyse

Werden Daten mittels eines automatischen Programms herunterladen, wird dieses Programm unter Umständen den von der SSL-Analyse ausgetauschten Datenschlüssel nicht akzeptieren und dies als Fehler interpretieren.

Dies geschieht meist dann, wenn das Programm den übergeben Datenschlüssel gegen eine eigene Datenbank prüft und dieser Datenbank der Atruvia-Datenschlüssel nicht bekannt ist (https://de.wikipedia.org/wiki/HTTP_Public_Key_Pinning). In diesem Fall können Sie die entsprechende Datenverbindung über einen Eintrag in der Whitelist von der SSL-Analyse ausnehmen.

Alternativ sollten Sie prüfen, ob es möglich ist, in Ihrem Programm entweder die Schlüsselprüfung zu deaktivieren oder den Schlüssel von Atruvia in die Schüsseldatenbank des Programms zu importieren.

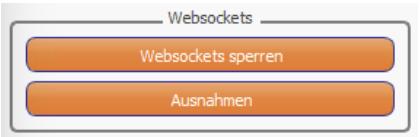
4.8.3 SSL-Analyse

Unter diesem Menüpunkt können Sie für das ausgewählte Profil die SSL-Analyse ein und ausschalten.

4.8.4 Ausnahmen

Hier können Sie gezielt Adressen/Ziele aus der SSL-Analyse ausschließen.
Beispiele für die Verwendung finden sie im Kapitel 4.2 Das Listen-Prinzip.

4.9 Websockets



Weiterführende Informationen zu Websockets finden Sie hier:
https://de.wikipedia.org/wiki/WebSocket

4.9.1 Websockets sperren

Unter diesem Menüpunkt können Sie für das ausgewählte Profil die Websockets ein- und ausschalten.

4.9.2 Ausnahmen

Hier können Sie gezielt Adressen oder Ziele für den Zugriff mittels Websockets freigeben. Beispiele für die Verwendung finden sie im Kapitel 4.2 Das Listen-Prinzip.

4.10 Uploadfilter

4.10.1 Uploads sperren

Hier können Sie den Upload von Dateien für alle Benutzer eines Profils sperren, sofern ein Upload eindeutig erkannt wurde. Bitte beachten Sie, dass die Uploadsperre bei verschlüsselten Zielen nur mit aktivierter SSL-Analyse funktional ist. Uploads, die außerhalb des Internetstandards implementiert wurden, werden u.U. nicht erkannt.

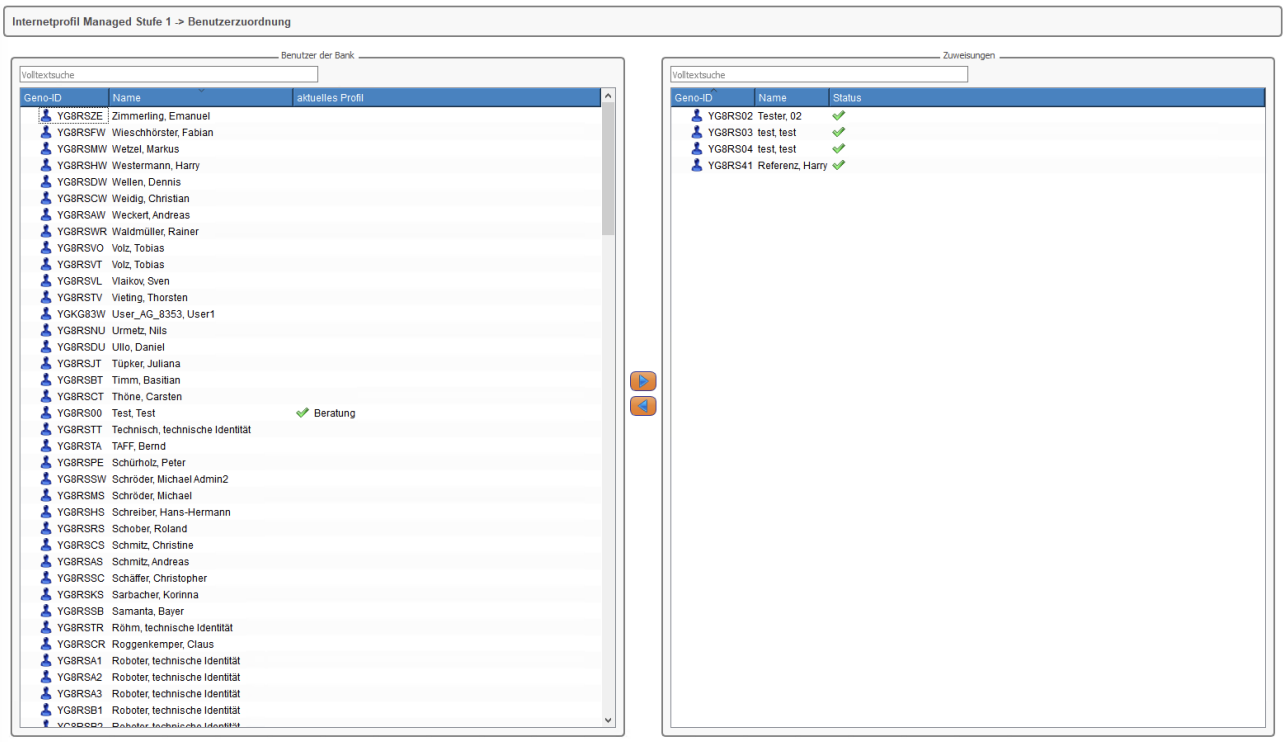
4.10.2 Ausnahmen

Hier können Sie Ziele anhand des Hostnamens (z. B. wetter.de) von der Uploadsperre ausnehmen. Hierdurch werden Subdomains wie pollenflug.wetter.de ebenfalls freigegeben. Die Freigabe von Zielen inklusive Pfadangaben wie zum Beispiel pollenflug.wetter.de/vorhersage ist nur mit aktivierter SSL - Analyse funktional.

4.11 Benutzerzuordnung

Die Zuordnung von Benutzern zu Internetprofilen erfolgt in SAGA im jeweiligen Profil.
Wählen Sie dazu linken Spalte der Benutzerzuordnung einen oder mehrere Benutzer aus und klicken sie die Pfeiltaste zur Zuweisung an. Die Benutzer befinden sich nun in der rechten Spalte der Benutzerzuordnung. Durch Speichern wird die Änderung beauftragt.

Ist ein Benutzer bereits einem Internetprofil zugeordnet, wird dies durch einen grünen Haken symbolisiert. Soll ein Benutzer einem anderen Internetprofil zugewiesen werden, wird die aktuelle Zuordnung gelöscht und der Benutzer dem neu ausgewählten Profil zugeordnet.



Standardmäßig findet die Authentifizierung am Atruvia Secure Webgateway automatisch und verschlüsselt über ein Kerberos-Ticket statt, das bei der Windows-Anmeldung generiert wird.

Schlägt die Benutzerauthentifizierung fehl oder wurde einem Benutzer kein Internetprofil zugewiesen, werden die entsprechenden Aufrufe gesperrt.

4.12 Globale Einstellungen

4.12.1 Sperren

Unter diesem Menüpunkt können Sie für ihr Institut bestimmte Ziele sperren. Diese Sperre wirkt global, unabhängig vom Benutzer oder dem zugeordneten Internetprofil.
Beispiele für die Verwendung finden sie im Kapitel 4.2 Das Listen-Prinzip.

4.12.2 Freischaltungen

Unter diesem Menüpunkt können Sie für ihr Institut bestimmte Ziele freigeben. Diese Sperre wirkt global unabhängig vom Benutzer oder dem zugeordneten Internetprofil oder gesperrten Kategorien.
Eine Freigabe über diesen Menüpunkt führt dazu, dass hier hinterlegte URLs von jeglicher Sperre am Atruvia Secure Webgateway ausgenommen werden. D.h. für hier gelisteten URLs sind die Funktionen Kategorie-, Reputations-, Medientyp-filter, Malware/Antivirusprüfung SSL-Scanning, Websocketsperre und Proxyauthentifizierung deaktiviert. Fügen Sie hier nur Websites ein, denen Sie vertrauen.
Möchten Sie nur einzelne Funktionen deaktivieren so nutzen Sie den Menüpunkt „Ausnahmen“ je Internetprofil.
Beispiele für die Verwendung finden sie im Kapitel 4.2 Das Listen-Prinzip.

4.12.3 Antivirus-Ausnahmen

Unter diesem Menüpunkt können Sie für ihr Institut bestimmte Ziele von der Malware/Antivirusprüfung ausschließen. Diese Liste wirkt global unabhängig vom Benutzer oder dem zugeordneten Internetprofil.
Beispiele für die Verwendung finden sie im Kapitel 4.2 Das Listen-Prinzip.

4.12.4 Authentifizierungsausnahmen

4.12.5 Authentifizierungsausnahmen Quelle

Hier können Sie einzelne Quell-IP-Adressen in Ihrem Haus von der Proxyauthentifizierung ausschließen. Diese Liste wirkt global unabhängig vom Benutzer oder dem zugeordneten Internetprofil.

Da ohne aktive Benutzerauthentifizierung kein Internetprofil zugeordnet werden kann, greift in diesem Fall das Internetprofil 0: keine Authentifizierung.

4.12.6 Authentifizierungsausnahmen Ziel

Unter diesem Menüpunkt können Sie für ihr Haus bestimmte Ziele von der Proxyauthentifizierung ausschließen. Diese Liste wirkt global unabhängig vom Benutzer oder dem zugeordneten Internetprofil.

Da ohne aktive Benutzerauthentifizierung kein Internetprofil zugeordnet werden kann, greift in diesem Fall das Internetprofil 0: keine Authentifizierung.

Achtung: Ohne eine aktive Benutzerauthentifizierung kann nicht geprüft werden, ob ein Benutzer überhaupt einem Internetprofil zugeordnet ist. Daher können auch Benutzer ohne zugewiesenes Internetprofil auf von der Proxyauthentifizierung ausgenommene Websites zugreifen. Auch diese werden dann Internetprofil 0 zugewiesen.

4.12.7 Basisauthentifizierung

Unterstützt eine Ihrer Anwendungen keine Kerberos-Authentifizierung, findet automatisch eine Rückstufung (Fallback) auf die sogenannte Basic Authentication (BasicAuth) statt. Hier müssen die Benutzerinformationen (inkl. Passwort) von Hand eingegeben werden und werden nicht verschlüsselt übermittelt. Daher ist BasicAuth standardmäßig deaktiviert.

Unter diesem Menüpunkt können sie die Basisauthentifizierung für ihr Institut aktivieren.

5 Reporting

5.1 Änderungsprotokoll

Über diese Schaltfläche können Sie das Protokoll der administrativen Tätigkeiten einsehen, die an den Einstellungen für Ihr Institut vorgenommen wurden. Das Protokoll enthält für jede Änderung den Zeitstempel, die Benutzerkennung des Anwenders, der die Änderungen vorgenommen hat, das betroffene Profil, die Kategorie der Tätigkeit und eine Textbeschreibung der Änderung.

Über das Kontext-Menü (Rechtsklick) können Sie das Protokoll kopieren oder als CSV-Datei lokal abspeichern.

5.2 Export von Einstellungen

Über diese Schaltfläche können Sie ein Protokoll der aktuellen Einstellungen für Ihr Institut als CSV-Datei erzeugen und lokal abspeichern.

5.3 Export von Benutzerzuordnungen

Über diese Schaltfläche können Sie die aktuellen Benutzerzuordnungen zu den einzelnen Profilen für Ihr Institut als CSV-Datei erzeugen und lokal abspeichern.

5.4 Export von Konfigurationsinhalten

Um einzelne Konfigurationsinhalte (z. B. alle gesperrten Adressen eines Profils) zu exportieren, können Sie innerhalb der Anzeige der Konfigurationsinhalte über das Kontext-Menü „Export in Zwischenablage“ oder „Export in CSV“ auswählen.

5.5 Import von Konfigurationsinhalten

Sollte es nötig sein, mehrere Konfigurationsinhalte auf einmal zu importieren, so ist dies innerhalb der Anzeige der entsprechenden Konfigurationsinhalte (z. B. Adresse) über das Kontext-Menü (Rechtsklick) „Hinzufügen aus Zwischenablage“ und „Hinzufügen aus CSV“ möglich.

Bitte beachten Sie dabei, dass aus der Zwischenablage lediglich Werte, aber keine Kommentare eingefügt werden können. Mehrere Werte trennen Sie bitte mit Zeilenumbrüchen.

Ein Import über eine CSV-Datei darf auch Kommentare enthalten. Werte und Kommentare trennen Sie bitte mit einem Semikolon.