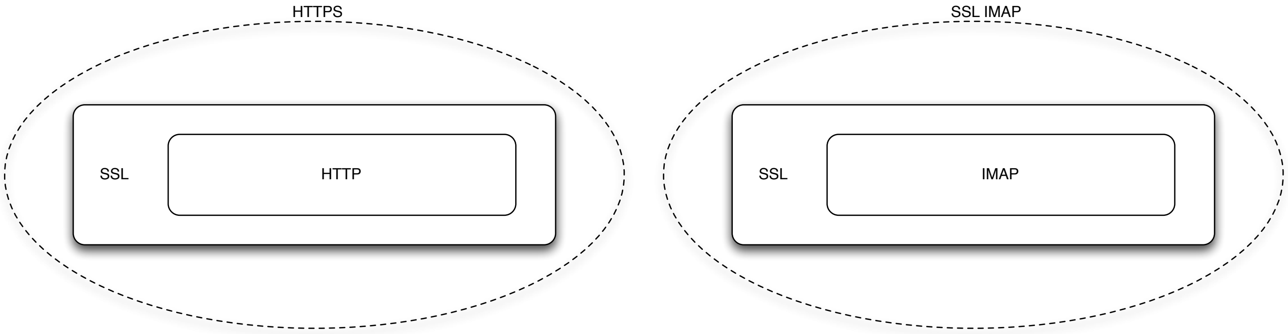
Controlling SSL Decryption

Tech Note

Overview

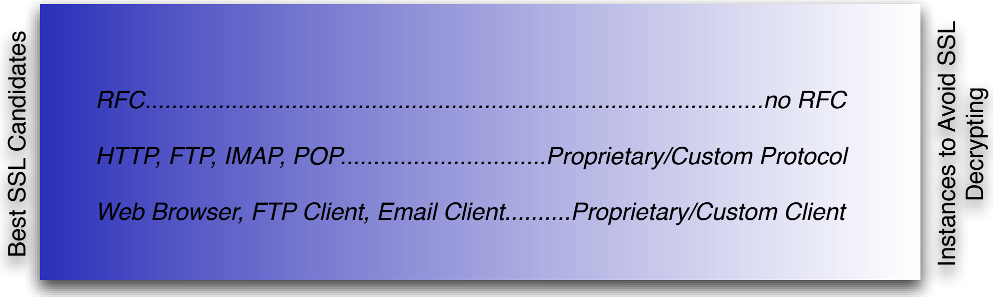
SSL Decryption is a key feature of the PA-4000 Series firewall. With it, SSL-encrypted traffic is decrypted for visibility, control, and granular security. App-ID and the Antivirus, Vulnerability, Anti-Spyware, URL Filtering, and File-Blocking Profiles are applied to decrypted traffic before being re-encrypted as traffic exits the device. End-to-end SSL security between clients and servers is maintained while that PA-4000 Series acts as a trusted third party during the connection. No decrypted traffic leaves the device.

A handful of networking vendors inspect SSL encrypted HTTP traffic (HTTPS). Palo Alto Networks goes further by inspecting compliant SSL traffic, no matter the protocol encapsulated by it. The figure below shows how SSL encapsulates HTTP and IMAP traffic to give HTTPS and SSL IMAP. Palo Alto Networks devices understand SSL, and can 'unwrap' the encapsulation to expose the underlying protocol and applications.



SSL Variability

Various applications and clients use SSL encryption. When web servers communicate with web browsers via HTTPS, the SSL highly conforms to the SSL RFCs. Standardization is key to making sure services are available to anyone on the Internet with a web browser.


Best SSL Candidates
RFC...no RFC
HTTP, FTP, IMAP, POP..............................Proprietary/Custom Protocol
Web Browser, FTP Client, Email Client..........Proprietary/Custom Client
Instances to Avoid SSL Decrypting

That is not the case with other uses of SSL or encryption, such as:

- Encrypted communications between a proprietary client/server application
  - management consoles for networking equipment
  - non-browser-based clients used for proprietary applications
- Evasive Applications
  - Skype
  - bitTorrent
- SSL VPNs

Application that are not required to interoperate with off-the-shelf clients may deviate enough from the SSL standard or typically available options such that they no longer works when decrypted with a PA-4000 Series firewall.

Examples of deviations from the SSL standards or common configurations options are:

- use of proprietary or nonstandard encryption methods
- client software coded to accept traffic from specific certificates (Windows Update)
- client software unable to add new trusted certificate authorities

Applications use various degrees of SSL for tunneling, privacy, and authentication. Unfortunately, some are not implemented to standards or use capabilities in the standards that are not compatible with Palo Alto Networks SSL decryption capability. In addition, SSL decryption cannot be used when servers require client certificates.

When first implementing SSL decryption we recommend a targeted approach to avoid breaking applications that do not successfully decrypted. Please note that the below recommendations are the starting point. More aggressive policies can be implemented once the base policy is in place and the full range of applications on the network known.

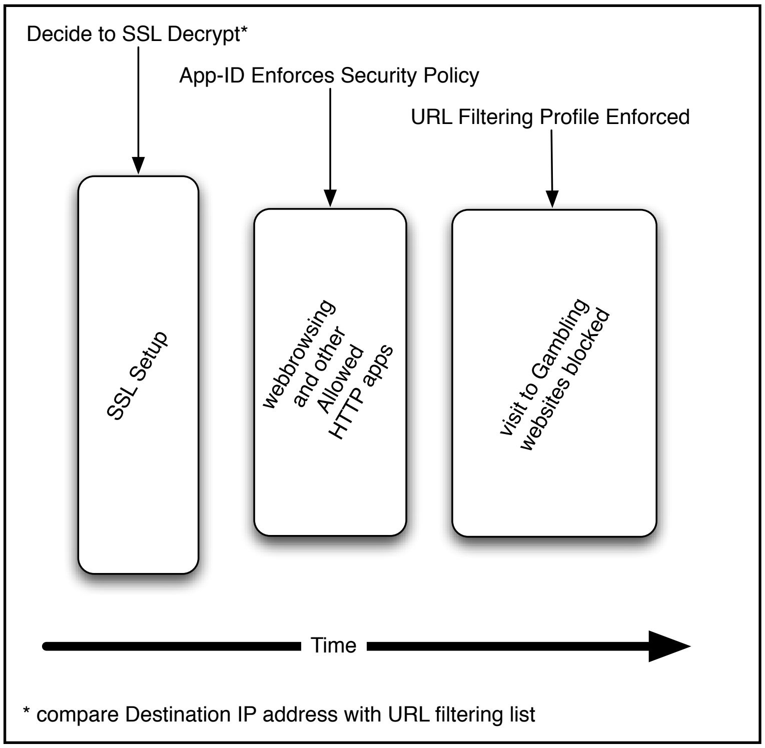
When SSL Decryption Is Not a Good Choice

- Server requires client certificates
- Non-standard implementations of SSL used
- New certificate authorities can’t be added to the client application
- Client software requires specific server certificates

URL Filtering and SSL Decryption

URLs are not visible unless traffic is decrypted.

The SSL Decryption Policy uses URL filtering to decide which traffic to decrypt or not decrypt. User or destination address can also be used for the decryption decision, but in practice the decision is made on the URL filtering category of the destination address. The destination IP address is compared since the URL is not visible. The graphic to the right depicts this relationship.


Decide to SSL Decrypt*
App-ID Enforces Security Policy
URL Filtering Profile Enforced
SSL Setup
webbrowsing and other Allowed HTTP apps
visit to Gambling websites blocked
Time
* compare Destination IP address with URL filtering list

Decrypted traffic can take full advantage of App-ID along with the Antivirus, Vulnerability, Anti-Spyware, URL Filtering, and File-Blocking Profiles.

The Security Policy uses the actual URLs within decrypted HTTPS requests against the URL Filtering Profile. URL filtering is an action in the Security Policy, instead of a match criteria as in the SSL Decryption Policy.

In the table below, note how URL filtering is used in a different capacity depending on the Rulebase.

Rulebase	Match By	Action	Profile Enforced
SSL	IP Address/User/ **URL filtering** category of IP Destination Address	Decrypt	*n/a*
		No-Decrypt	
Security	IP address/User/App-ID/Service	Allow	**URL Filtering** Allows & Blocks
		Deny	*n/a*

As mentioned previously, some traffic may not decrypt successfully and should be avoided. Also, organizations may chose not to decrypt specific applications because they feel those destinations are trusted and pose less of a risk.

SSL traffic that is not decrypted renders the URL unreadable. In this case, the Security Policy checks the destination IP address against the URL filtering list to determine the correct Security Rulebase action.

Deciding Your SSL Decryption Policy

To determine your initial SSL Rulebase, focus on the applications you want to control and the URL filtering categories those might be classified under.

Answer the following:

- What applications to block?
- What URL filtering categories will those applications most likely be categorized in?

Do not decrypt the URL categories *unknown* or *infrastructure* when first deploying your PA-4000 Series firewall. *unknown* includes many non-HTTP applications, some of which will **not** correctly SSL decrypt. *infrastructure* includes the Windows Update service, which requires specific server certificates from Microsoft.

For an example, perhaps we want to control webmail, instant messages, and file transfers even when encrypted. To decrypt nearly all HTTPS traffic that contains these applications, the following categories should be set to decrypt in your SSL Rulebase:

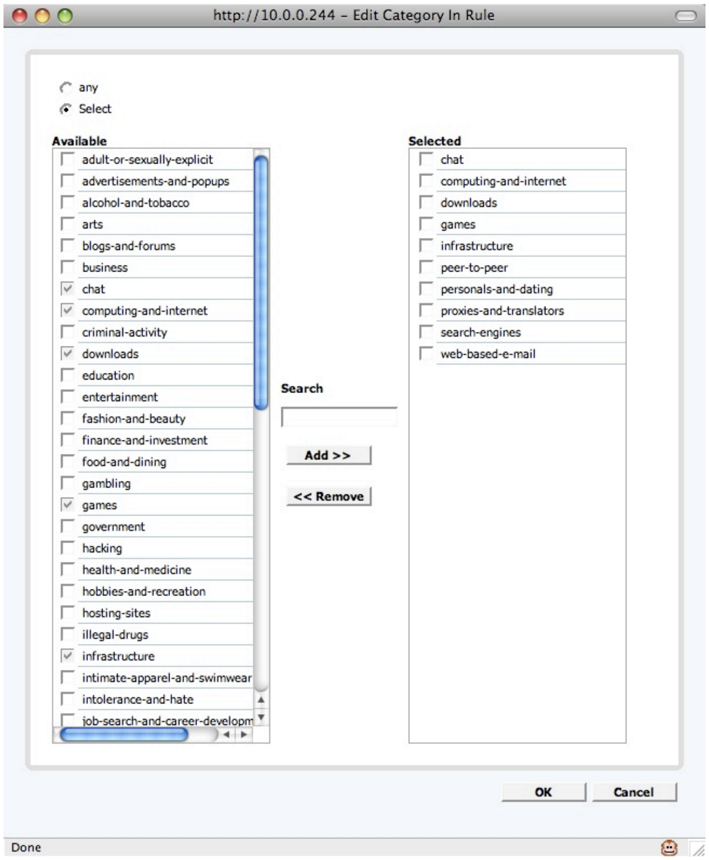
1. *web-based-e-mail* and *chat*
   - Covers point-web-based applications like Meebo
2. *search-engines*
   - Covers applications run by the big search engine companies like Google, Yahoo, Microsoft, and AOL
3. *peer-to-peer*
   - Covers peer-to-peer sites as well as some of the file sharing sites like foldershare
4. *downloads*
   - Includes many of the file sharing applications not captured by peer-to-peer, such as megaupload
5. *personals-and-dating* and *games*
   - Covers many of the web 2.0 mashups like myspace and facebook that have mail, im, and file transfer capabilities
6. *proxies-and-translators*
   - Covers many of the sites that are designed to tunnel other applications inside SSL
7. *computing-and-internet*
   - Covers several miscellaneous applications

Initial SSL Decryption Policy

Now that we have a list of URL filtering categories to target, we are ready to create our SSL Decryption rulebase.

To decrypt just the needed SSL traffic, do the following:

- In the Policies Tab, select the SSL Decryption option from the left hand menu
- Add in a rule from your Trust to your Untrust network
- In the rule just added, select 'any' in the category column of the rule
- Select the previously determined categories from the left hand side of the list, then click Add
- Change the action of the rule to decrypt.
- Commit your policy



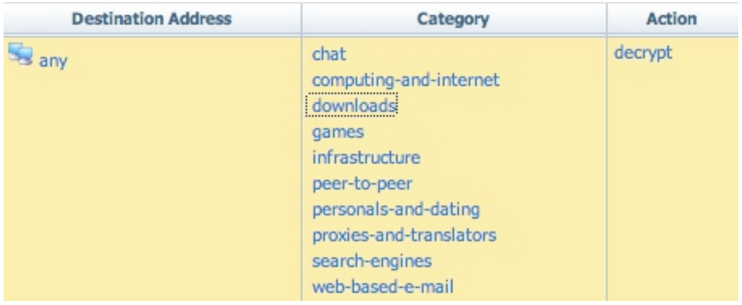
○ any
● Select

Available

- □ adult-or-sexually-explicit
- □ advertisements-and-popups
- □ alcohol-and-tobacco
- □ arts
- □ blogs-and-forums
- □ business
- ☑ chat
- ☑ computing-and-internet
- □ criminal-activity
- ☑ downloads
- □ education
- □ entertainment
- □ fashion-and-beauty
- □ finance-and-investment
- □ food-and-dining
- □ gambling
- ☑ games
- □ government
- □ hacking
- □ health-and-medicine
- □ hobbies-and-recreation
- □ hosting-sites
- □ illegal-drugs
- ☑ infrastructure
- □ intimate-apparel-and-swimwear
- □ intolerance-and-hate
- □ job-search-and-career-developm

Selected

- □ chat
- □ computing-and-internet
- □ downloads
- □ games
- □ infrastructure
- □ peer-to-peer
- □ personals-and-dating
- □ proxies-and-translators
- □ search-engines
- □ web-based-e-mail



Destination Address	Category	Action
any	chat computing-and-internet downloads games infrastructure peer-to-peer personals-and-dating proxies-and-translators search-engines web-based-e-mail	decrypt

At this point, the decrypted traffic will be checked against the Security Policy. The traffic can be controlled by App-ID or checked with the Antivirus, Vulnerability, Anti-Spyware, URL Filtering, and File-Blocking Profiles with rules in the Security Policy.

Advanced SSL Decryption Policies

The previous policy provides very good SSL decryption coverage while minimizing tuning and customization of the SSL decryption policy. To slowly make this policy more aggressive, start by monitoring the traffic logs for port 443. Create exception (do-not-decrypt) policies for trusted company applications that are running over SSL. These would include applications like Salesforce.com, accounting software, or web conferencing tools. Once in place, add more categories to the decrypt list.