Check Point Configuration with Radware (Alteon) SSL Decrypt with URL/UserCheck Functionality

Mike Walsh
Security Engineer, US Central
December 21, 2018

Contents

Check Point/Radware Design Goal

The goal of this design was to facilitate the use of Radware/Alteon devices to decrypt SSL traffic and redirect it to Check Point for advanced inspection. This inspection included the use of Check Point URL filtering which was configured to provide a UserCheck page to the end user. The flow is described as follows:

Client -> Alteon (HTTPS) 443 -> Alteon (HTTP) 8080 -> Check Point FW (HTTP) 8080 -> Alteon (HTTP) 8080 -> Alteon (HTTPS) 443 -> Server 443

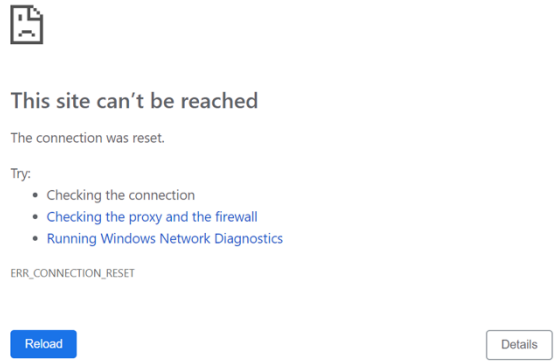
Check Point URL Filtering

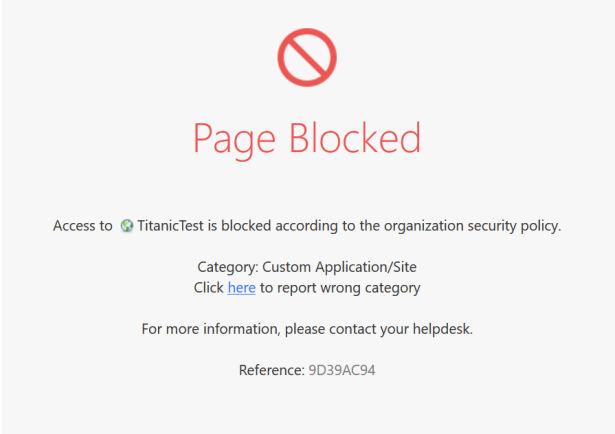
Check Point has included web filtering with its security gateways for many years. URL Filtering is a standard blade included with all Next Generation Threat Prevention (NGTP) and Next Generation Threat Extraction (NGTX) packages. As is common with most major web filtering vendors, Check Point tracks over 200 million websites and categorizes them into 70+ categories for easy identification and policy configuration. These categories are typically used in the Access Control policy to Block and/or Allow websites by their category tags, with specific sites being identified by the creation of Custom Site to allow for policy exceptions to the general category, or for categorization override. An example URLF policy for Check Point R80.10 is shown here:

No.	Name	Source	Destination	Services & Applications	Content	Action	Track
5	Access to Internet according to Web control policy	InternalZone	Internet	Any	Any	Web Control	N/A
5.1	Block abuse/ high risk applications	Corporate LANs Branch Office LAN	Internet	Child Abuse Gambling High Risk Pornography Spyware / Malicious Sites	Any	Drop Blocked Message -...	Log
5.2	HR can access to social network applications	HR	Internet	Social Networking	Any	Inform Access Approval Once a day Per application/site	Log Accounting
5.3	All employees can access YouTube for work purposes	Corporate LANs Branch Office LAN	Internet	YouTube - Custom Site	Any	Ask Company Policy Once a day Per application/site	Log
5.4	Block specific URLs	Any	Internet	Blocked URLs	Any	Drop	Log
5.5	Block specific categories for all employees	Corporate LANs Branch Office LAN	Internet	Social Networking Streaming Media Protocols P2P File Sharing	Any	Drop Blocked Message -...	Log
5.6	Cleanup	Any	Any	Any	Any	Accept	Log

Problem Description

In testing the design in our customers environment, we came across an issue where traffic that was sent from the end user through Alteon A to the Check Point firewall returned a “This site can’t be reached” page to the end user as opposed to the configured UserCheck block page.

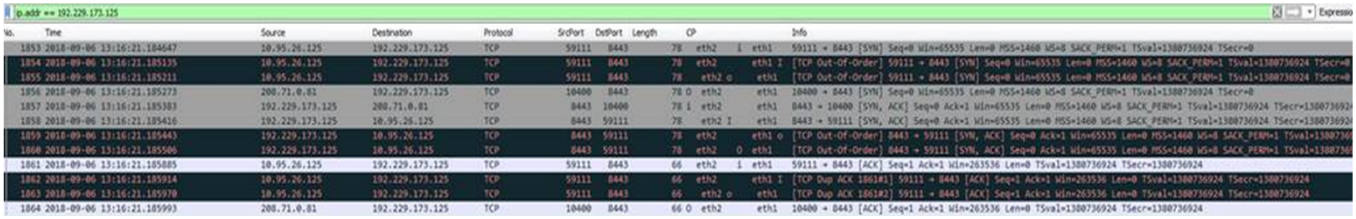




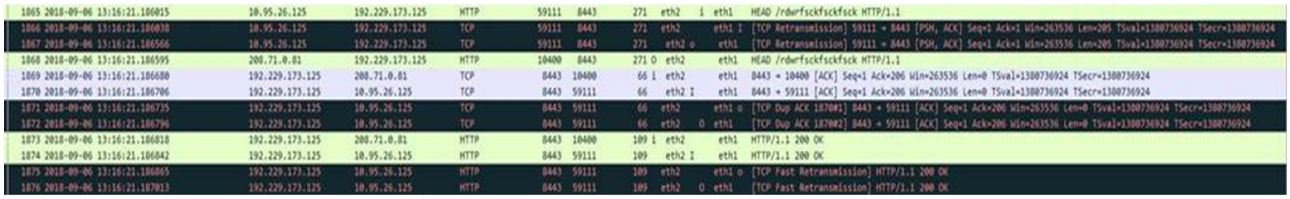
Troubleshooting/Problem Determination

Working with the customer and Radware we took the following Wireshark Capture and provided this analysis.

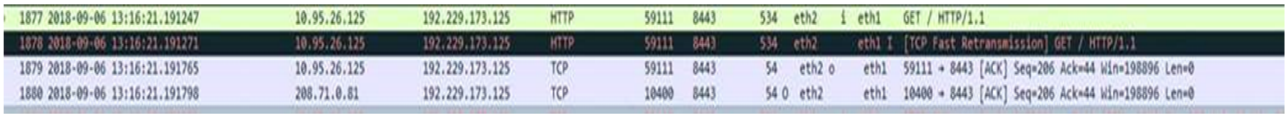
1. Three way handshake is completed, we can see all four stages on the CP gateway (‘i’, ‘I’, ‘o’ and ‘O’) from the internal interface eth1 to the external interface eth2 and vice versa:



2. HEAD, ACK and HTTP 200 OK packets pass through the gateway:



3. However when the gateway gets the GET packet it doesn’t pass through, instead the gateway sends an ACK to the website:



4. Looking at the debugs I can see that the CP gateway is stopping the connection and trying to inject the block page. I also see that it vanishes the original packet and sends ACK to the server instead:

; 6Sep2018 17:16:21.191635;[cpu_6];[fw4_2];psl_set_server_injection_ex: setting injection to connection <dir 1, 10.95.26.125:59111 -> 192.229.173.125:8443 IPP 6>;
; 6Sep2018 17:16:21.191637;[cpu_6];[fw4_2];psl_set_reject_conn: added reject dirs 1 to astream=fffc20091226570 (flags 0x40448c1/0xd27/0xd07);
; 6Sep2018 17:16:21.191639;[cpu_6];[fw4_2];psl_process_data: processing function for app 3[HTTP_DISPATCHER] returned STOP_AND_INJECT;
; 6Sep2018 17:16:21.191706;[cpu_6];[fw4_2];psl_handle_segment_injection_tcp: vanishing original packet and sending stripped (ack-only) packet.;

5. It looks like it timed out waiting for the internal server to launch the block page:

; 6Sep2018 17:16:22.231583;[cpu_6];[fw4_2];psl_update_segment_injection_cb: server idle timeout reached at time 1536254182;

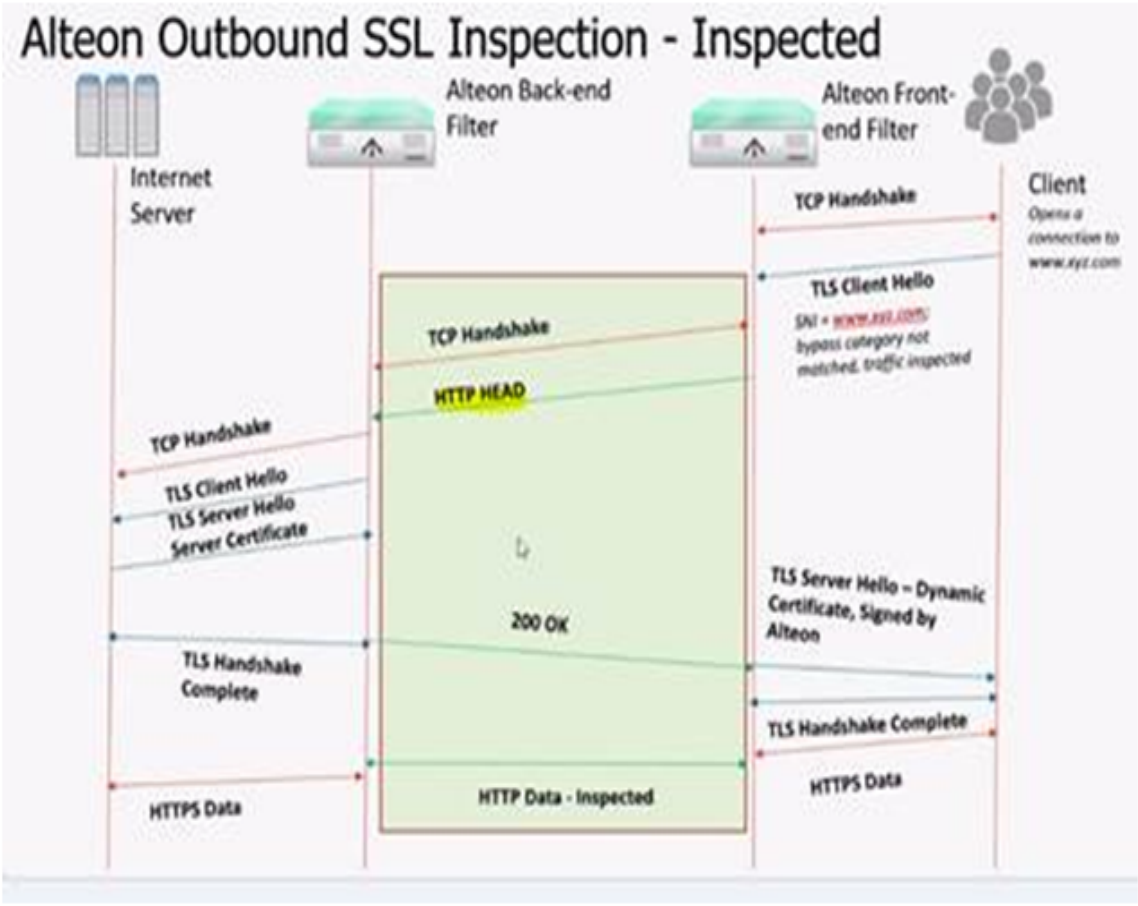
6. Then after a second the client PC (or Radware device) sends a retransmission packet of the GET command (PSH,ACK) and right after the gateway sends RST packets to both client and server:

7. When the gateway sees the retransmission, it drops the packet and attempts to inject the block page again, however aborts because it was already done and therefore sends the RST packets to both client and server:

6Sep2018 17:16:22.231585;[cpu_6];[fw4_2];psl_can_send_injection_ex: already passed packets on injected direction, aborting injection;
; 6Sep2018 17:16:22.231585;[cpu_6];[fw4_2];psl_verify_can_send_injection: sending RST to client and server;

In working with Check Point R&D it was determined that the Gateway was behaving as designed and that the issue matched the below SK. The issue relates to the requirement that Radware has in the order at which it sends HEAD requests between Alteon devices. This requirement is proprietary to Radware. The customer was also testing A10 and F5 and we did not have this issue.

SK108312 - *When browsing to a page blocked by Application Control policy, the block page is displayed only occasionally*



Since this packet is passed first (not expected in regular HTTP traffic), then when the CP gateway sees the GET packet it attempts to inject the UserCheck page but aborts because the connection already passed the HEAD packet:

> ; 6Sep2018 17:16:22.231585;[cpu_6];[fw4_2];psl_can_send_injection_ex: already passed packets on injected direction, aborting injection;

Kernel Parameter Workaround

Per SK108312 there is a kernel parameter that can be set to allow the gateway to accept the order of packets required by Radware (command below). However, this opens a security vulnerability on the gateway. Check Point recommends usage of the kernel parameter for testing only.

```
fw ctl set int psl_verify_segment_injection = 0
```

Check Point Hotfix

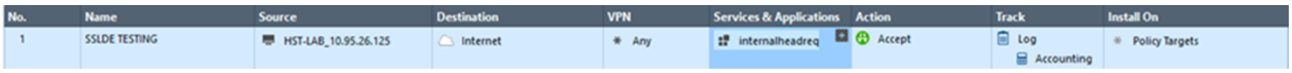
Working with Check Point R&D, they produced the following Hotfix - HOTFIX_R80_10_JHF_142_281 to be installed on top of JHF142 for R80.10 which the customer has deployed. This patch, while it does not set the above kernel parameter it does allow the gateway to handle specifically an out of order HTTP HEAD request and close the security vulnerability.

Radware URL Rule

Additionally, based on the gateway policy the HTTP HEAD was being blocked, this needs to pass through, the next request which is the actual client request needs to be redirected by the user check.

HEAD /internalheadreq HTTP/1.1 ← This HEAD method needs to be allowed always.
Connection: Keep-Alive
Host: radware.com
Server_name: radware.com
Server_port: 443
App_id: 4
Session_id: 25300
Certificate: Request

So, we created a URL Custom Site to allow the communication.



*/internalheadreq – this is the URL that needs to be allowed.

With these pieces in place we have a working solution with the Radware (Alteon SSL Offload) with URL filtering with UserCheck.

