ALTEON SSL INSPECTION

Alteon SSL Inspection

DEMO LAB GUIDE

Lab Owner: Sean Ramati

May 23, 2023

TABLE OF CONTENTS

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided “as is”. Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness or performance

GUIDE OVERVIEW

This guide outlines the SSL inspection demo lab environment and provides detailed instructions to running the demonstration.

As part of the demonstration we will show the following scenarios:

- SSL inspection with 3 security devices: TAP, ICAP, and NGFW.
- Bypassing SSL inspection based on hostname.
- Bypassing SSL inspection based on web category (Finance, News, etc.).
- Blocking traffic to a specific web category.

Scenario1: SSL inspection with 3 security devices

In this scenario, encrypted traffic from the LAN is directed to the Alteon device. The Alteon decrypts the traffic and then redirects the clear traffic to each security device in the flow. Once each device has inspected the traffic, the Alteon re-encrypts it before sending it out to the internet.

Scenario 2: Bypassing SSL inspection to a hostname

In this scenario, we demonstrate how to bypass SSL inspection for a specific host. Traffic destined for this host is sent directly to the default gateway, bypassing the security devices.

Scenario 3: Bypassing SSL inspection based on web category

In this scenario, we demonstrate how to bypass SSL inspection for a specific web category. Traffic that matches the category is sent directly to the default gateway, bypassing the security devices.

Scenario 4: Blocking website category using URL filtering

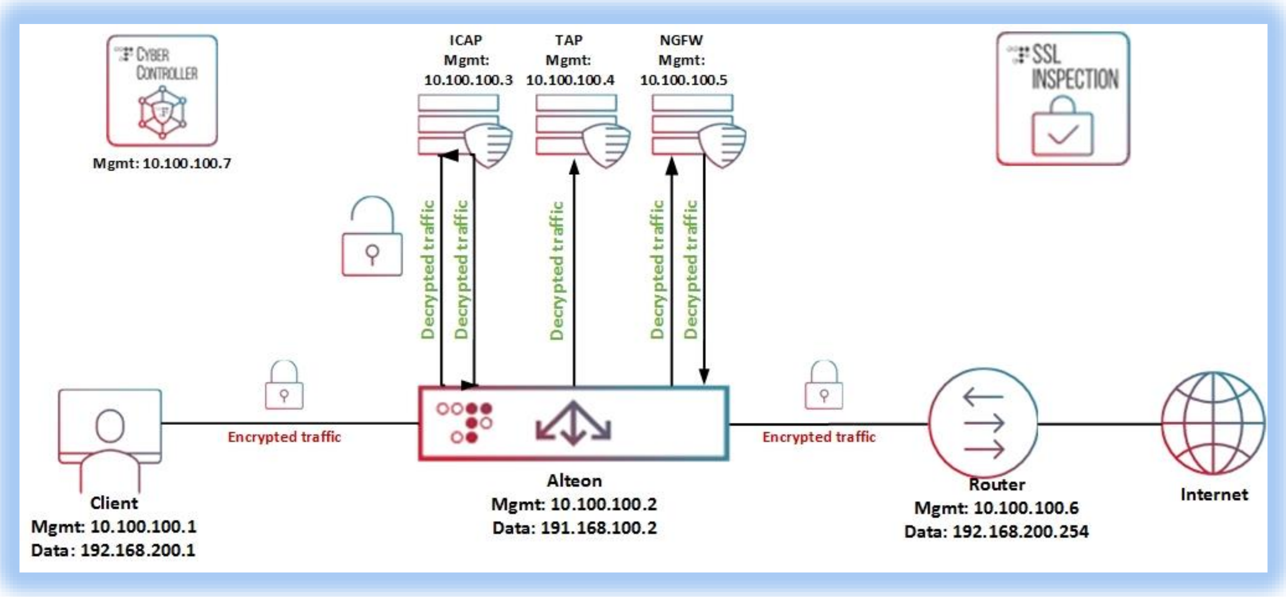
In this scenario, we demonstrate how to block a specific website category. Traffic from the configured category (News) is sent directly to the default gateway, and when traffic matches the relevant filter it is blocked.

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided “as is”. Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness or performance

Note:
For a more detailed description of the SSL Inspection solution please refer to Appendix A: SSL Inspection overview

LAB TOPOLOGY



The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided "as is". Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness or performance

1. Management Station

The Client PC serves as the management station for the setup. From this station, you can run the entire demo and access the following components:

- Alteon
- Vision
- Security devices
- Demo lab diagrams

This station is connected to the following networks:

1. Management network of the setup for managing the setup equipment.
2. Data network for client traffic.

2. Management Station Tools

The following tools are used on the Management Station in the demo lab:

- **Putty —** Used to connect the environment terminal connection.
- **Chrome browser —** Used to browse the internet through lab components.
- **Wireshark –** Used to open packet capture.

3. Verifying Alteon Configuration

Before running the demo, make sure to load the configuration to the device in order to ensure that it is configured correctly.

The configuration file is located on the desktop under the **Configuration** folder.

The file name is **Alteon.tgz**

4. Alteon Licnese

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided “as is”. Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness or performance

In case of license issues, please find below Alteon licenses:

- va-ngDlSwq1
- 1Gbps-6hCdnweN
- aas-slb-sslinsp-t3WIhyCA
- aas-ssl-Unlimited-dgN4QH89
- aas-perform-Uv9BRqYY
- aas-urlfilter-19oct2020-19nov2021-P3dhDnJJ

Note:

For detailed information on how to import the configuration please refer to Appendix B: Importing Alteon Configuration

5. IPs and Login Credentials

Component	*IP*	*User*	*Password*
Alteon	*10.100.100.2*	*radware*	*Radware1!*
Vision	*10.100.100.7*	*radware*	*Radware1!*
ICAP Server	*10.100.100.3*	*admin*	*radware*
TAP	*10.100.100.4*	*admin*	*radware*
NGFW	*10.100.100.5*	*admin*	*radware*
Router	*10.100.100.6*	*vyos*	*vyos*

RUNNING THE DEMO

During the demo you can use Wireshark to capture traffic on the Alteon and on the security devices. For detailed information on how to run Wireshark and how to explain the capture on the Alteon, refer to Appendix C: Running Packet Captures.

Note:

The client is configured to trust the Alteon as a Certificate Authority in order to avoid security alerts on the browser. For details on how to add the Alteon as a trusted CA refer to Appendix D: Adding the Alteon as a Trusted CA

Note:

Non-HTTPS traffic passes through the Alteon directly to the default gateway (ignoring the SSLi solution).

1. Scenario 1 – SSL Inspection Demo

In this scenario we demonstrate Alteon outbound SSL inspection core functionality:

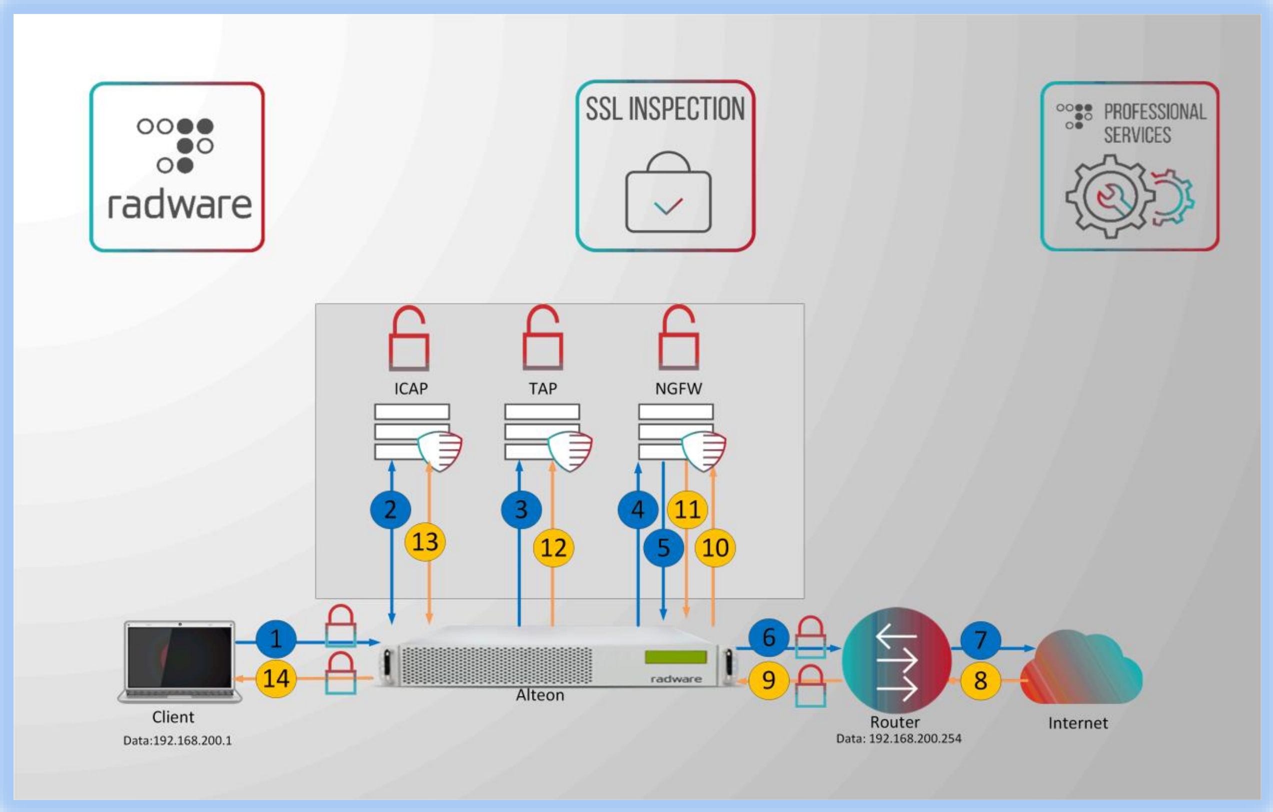
- Client sends HTTPS request to the internet
- The Alteon intercepts the traffic and performs the following:
  - Decrypt the HTTPS traffic.
  - Send the unencrypted traffic to the ICAP server for malicious object scanning.
  - Send a copy of the unencrypted traffic to the TAP device for recording.
  - Send the unencrypted traffic through NGFW for layer7 inspection.
  - Re-Encrypt the HTTP traffic.
  - Send the HTTPS traffic to the original destination website.

Note:

In order to view the Alteon configuration refer to Appendix E: Scenario 1 Configuration
Please Open SSL Inspection analytics using Appendix I: Vision SSL Inspection Analytics

Scenario 1 – Diagram and Traffic Flow

The diagram below details the entire flow of the traffic:



Note:

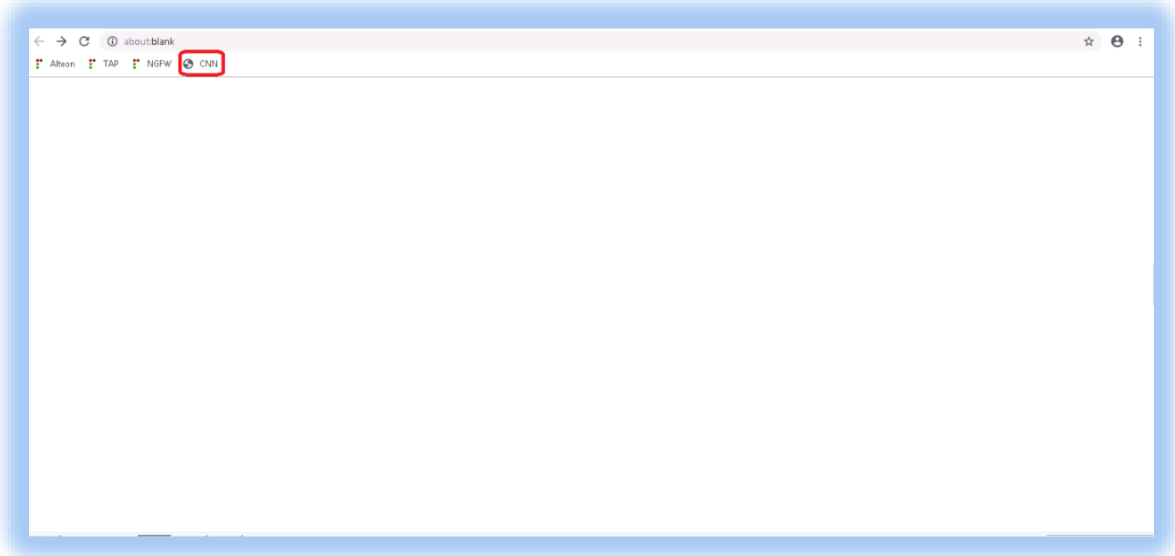
Lines in Blue represent requests to the internet

Lines in Orange represent responses from the internet

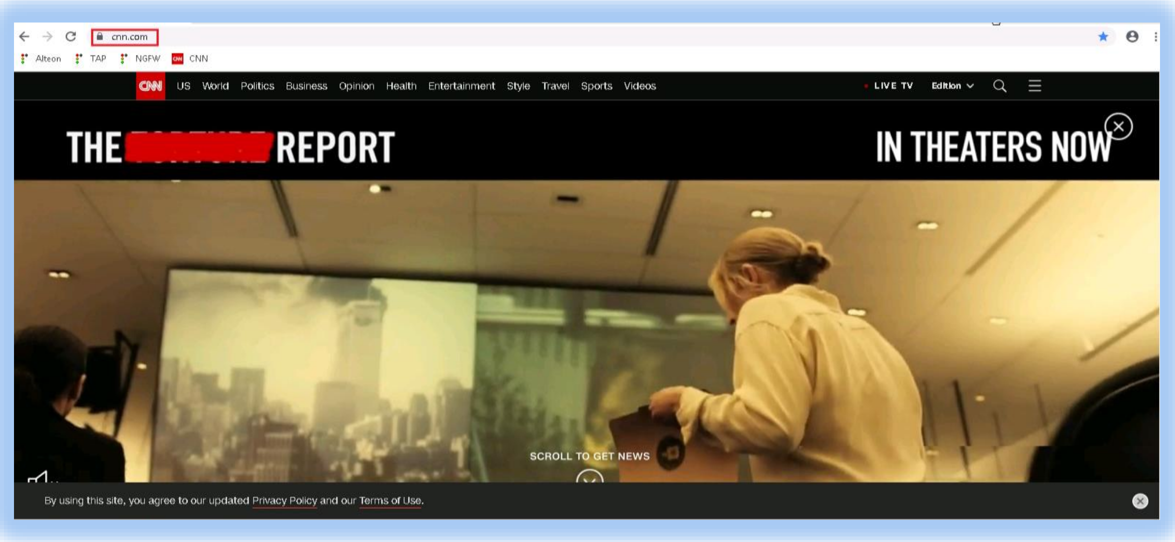
1. The Client sends request to an HTTPS web site
2. The Alteon decrypts the HTTPS traffic and sends the unencrypted HTTP request to the ICAP server over ICAP protocol. The ICAP responds to the Alteon with allow or block after finishing inspection.
3. The Alteon sends a copy of the request to the Tap device.
4. The Alteon sends the request to the NGFW.
5. The NGFW return inspected request to the Alteon.
6. The Alteon Re-encrypts the request and sends it to the router.
7. The Router performs NAT and forwards the request to the internet.
8. The Website sends the response to the router.
9. The Router sends the response to the Alteon.
10. The Alteon decrypts the HTTPS response and sends the unencrypted HTTP response to the NGFW.
11. The NGFW returns the inspected response to the Alteon.
12. The Alteon sends a copy of the response to the Tap device.
13. The Alteon sends the unencrypted HTTP response to the ICAP server over ICAP protocol. The ICAP responds to the Alteon with allow or block after finishing inspection.
14. The Alteon re-encrypts the response and sends it to the client

Running Scenario 1

1. Open **Chrome** browser and click on **CNN** bookmark:

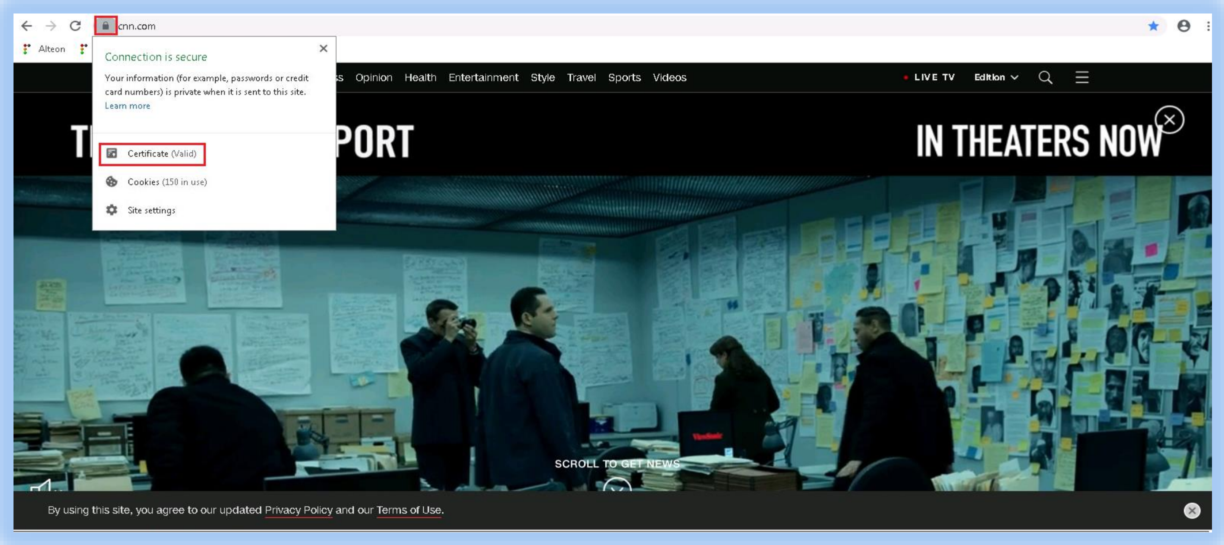


2. Click on the **Lock Button** and then **Certificate** to verify the certificate issuer:



By using this site, you agree to our updated Privacy Policy and our Terms of Use.

3. Click on **Certificate**:



Connection is secure

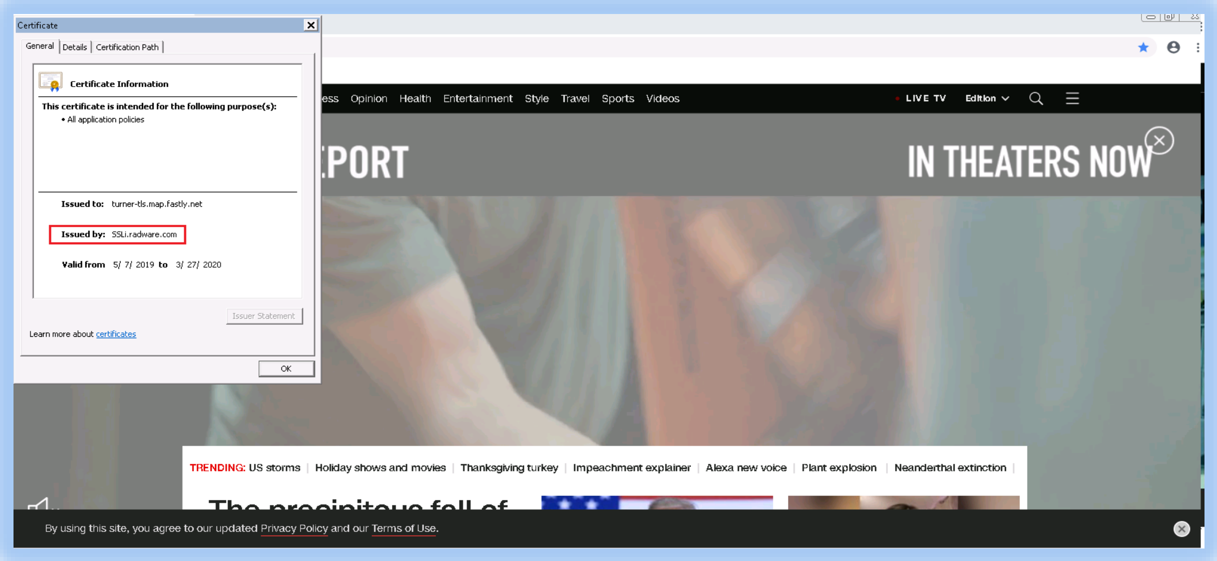
Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

Certificate (Valid)

Cookies (150 in use)

Site settings

4. We can see that the certificate was issued by the Alteon, meaning the traffic was forwarded to security devices for inspection and re-encrypted successfully:


Opinion
Health
Entertainment
Style
Travel
Sports
Videos
LIVE TV
Edition
IN THEATERS NOW
TRENDING: US storms | Holiday shows and movies | Thanksgiving turkey | Impeachment explainer | Alexa new voice | Plant explosion | Neanderthal extinction
By using this site, you agree to our updated Privacy Policy and our Terms of Use.

Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):
- All application policies

Issued to: turner-tls.map.fastly.net

Issued by: SSLi.radware.com

Valid from 5/ 7/ 2019 to 3/ 27/ 2020

Issuer Statement

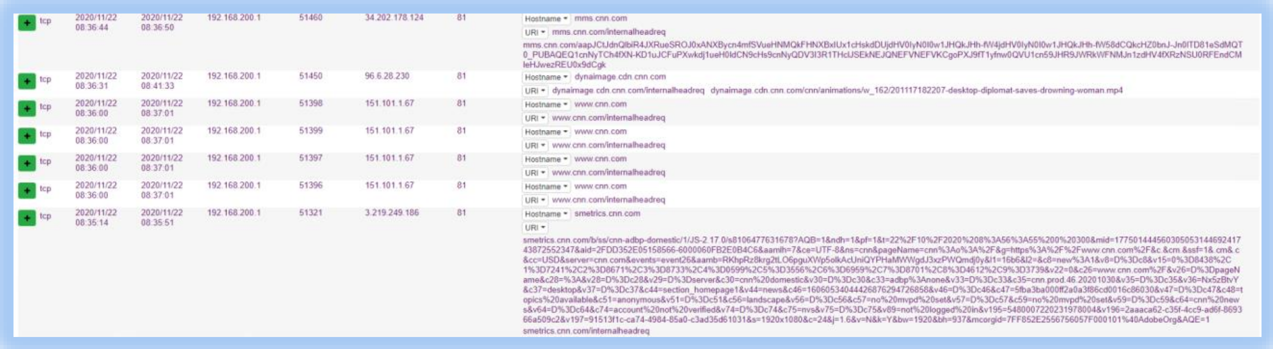
Learn more about certificates

OK

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

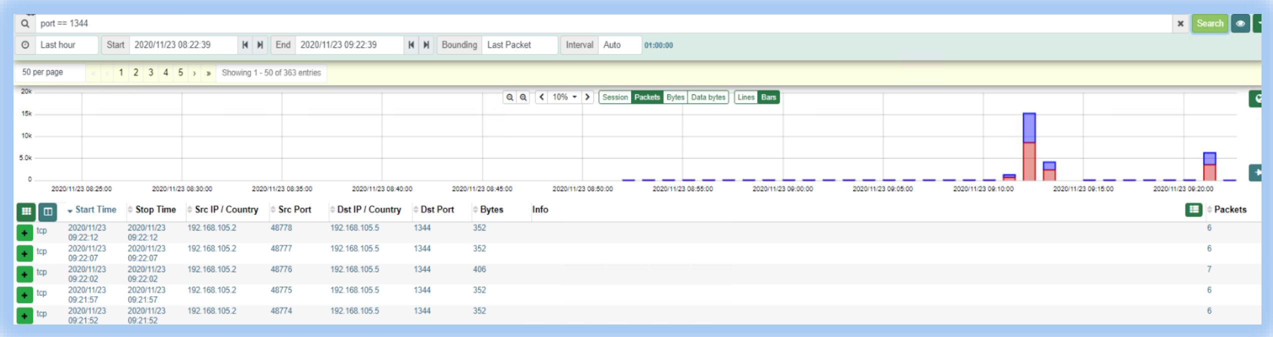
All information provided in the Demo lab and documentation is provided “as is”. Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness or performance

5. Browse to "TAP" bookmark in order to watch traffic reaching the "TAP" device:



+	tcp	2020/11/22 08:36:44	2020/11/22 08:36:50	192.168.200.1	51460	34.202.178.124	81	Hostname ▾ mms.cnn.com URI ▾ mms.cnn.com/internalheadreq mms.cnn.com/aapJCtJdnQlbiR4JXRueSROJ0xANXBycn4mfSVueHNMQkFHNXBxIUx1cHskdDUjdHV0lyN0l0w1JHQkJHh-fW4jdHV0lyN0l0w1JHQkJHh-fW58dCQkcHZ0bnJ-Jn0lTD81eSdMQT0_PUBAQEQ1cnNyTCh4fXN-KD1uJCFuPXwkdj1ueH0ldCN9cHs9cnNyQDV3I3R1THcUSEkNEJQNEFVNEFVKCgoPXJ9fT1yfnw0QVU1cn59JHR9JWRkWFNMJn1zdHV4fXRzNSU0RFEndCMleHJwezREU0x9dCgk
+	tcp	2020/11/22 08:36:31	2020/11/22 08:41:33	192.168.200.1	51450	96.6.28.230	81	Hostname ▾ dynaimage.cdn.cnn.com URI ▾ dynaimage.cdn.cnn.com/internalheadreq dynaimage.cdn.cnn.com/cnn/animations/w_162/201117182207-desktop-diplomat-saves-drowning-woman.mp4
+	tcp	2020/11/22 08:36:00	2020/11/22 08:37:01	192.168.200.1	51398	151.101.1.67	81	Hostname ▾ www.cnn.com URI ▾ www.cnn.com/internalheadreq
+	tcp	2020/11/22 08:36:00	2020/11/22 08:37:01	192.168.200.1	51399	151.101.1.67	81	Hostname ▾ www.cnn.com URI ▾ www.cnn.com/internalheadreq
+	tcp	2020/11/22 08:36:00	2020/11/22 08:37:01	192.168.200.1	51397	151.101.1.67	81	Hostname ▾ www.cnn.com URI ▾ www.cnn.com/internalheadreq
+	tcp	2020/11/22 08:36:00	2020/11/22 08:37:01	192.168.200.1	51396	151.101.1.67	81	Hostname ▾ www.cnn.com URI ▾ www.cnn.com/internalheadreq
+	tcp	2020/11/22 08:35:14	2020/11/22 08:35:51	192.168.200.1	51321	3.219.249.186	81	Hostname ▾ smetrics.cnn.com URI ▾ smetrics.cnn.com/b/ss/cnn-adbp-domestic/1/JS-2.17.0/s8106477631678?AQB=1&ndh=1&pf=1&t=22%2F10%2F2020%208%3A56%3A55%200%20300&mid=1775014445603050531446924174387255234 7&aid=2FDD352E05158566-6000060FB2E0B4C6&aamlh=7&ce=UTF-8&ns=cnn&pageName=cnn%3Ao%3A%2F&g=https%3A%2F%2Fwww.cnn.com%2F&c.&cm.&ssf=1&.cm&.c&cc=USD&server=cnn.com&events=event26&aamb=RKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y&l1=16b6&l2=&c8=new%3A1&v8=D%3Dc8&v15=0%3D8438%2C1%3D7241%2C2%3D8671%2C3%3D8733%2C4%3D0599%2C5%3D3556%2C6%3D6959%2C7%3D8701%2C8%3D4612%2C9%3D3739&v22=0&c26=www.cnn.com%2F&v26=D%3DpageName&c28=%3A&v28=D%3Dc28&v29=D%3Dserver&c30=cnn%20domestic&v30=D%3Dc30&c33=adbp%3Anone&v33=D%3Dc33&c35=cnn.prod.46.20201030&v35=D%3Dc35&v36=Nx5zBtvY&c37=desktop&v37=D%3Dc37&c44=section_homepage1&v44=news&c46=16060534044426876294726858&v46=D%3Dc46&c47=5fba3ba000ff2a0a3f86cd0016c86030&v47=D%3Dc47&c48=topics%20available&c51=anonymous&v51=D%3Dc51&c56=landscape&v56=D%3Dc56&c57=no%20mvpd%20set&v57=D%3Dc57&c59=no%20mvpd%20set&v59=D%3Dc59&c64=cnn%20news&v64=D%3Dc64&c74=account%20not%20verified&v74=D%3Dc74&c75=nvs&v75=D%3Dc75&v89=not%20logged%20in&v195=5480007220231978004&v196=2aaaca62-c35f-4cc9-ad6f-869366a509c2&v197=91513f1c-ca74-4984-85a0-c3ad35d61031&s=1920x1080&c=24&j=1.6&v=N&k=Y&bw=1920&bh=937&mcorgid=7FF852E2556756057F000101%40AdobeOrg&AQE=1 smetrics.cnn.com/internalheadreq

6. Browse to "ICAP" bookmark in order to watch traffic reaching the ICAP device and click the "+" button:



port == 1344

Last hour | Start 2020/11/23 08:22:39 | End 2020/11/23 09:22:39 | Bounding Last Packet | Interval Auto | 01:00:00

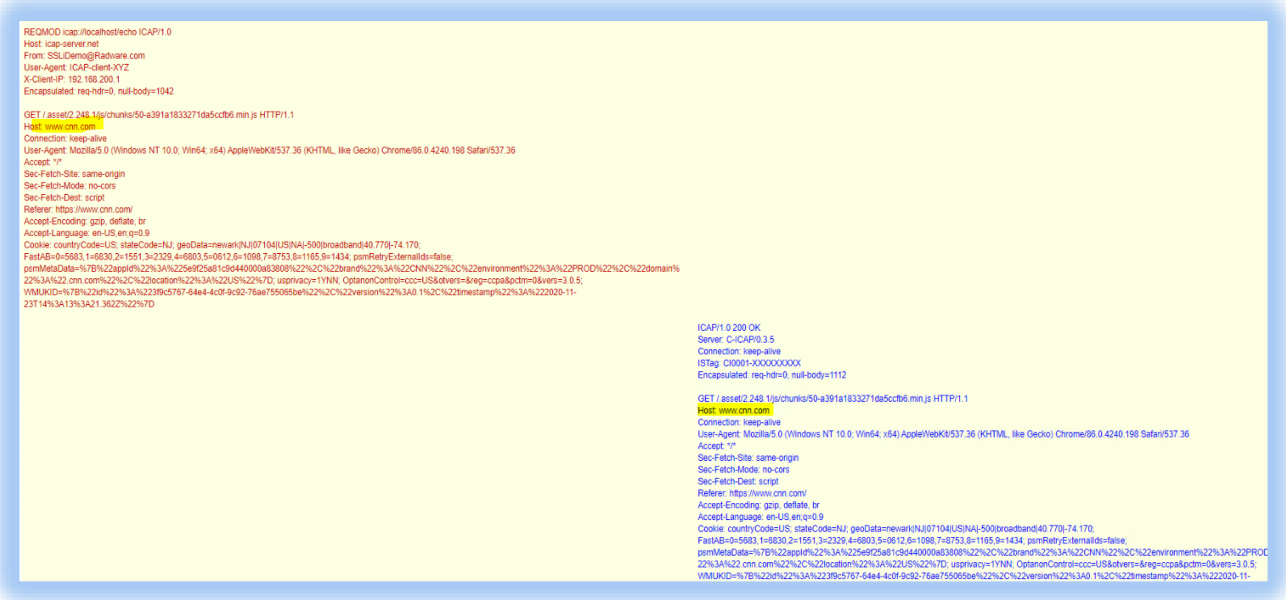
50 per page | « ‹ 1 2 3 4 5 › » | Showing 1 - 50 of 363 entries

	Start Time	Stop Time	Src IP / Country	Src Port	Dst IP / Country	Dst Port	Bytes	Info	Packets
+ tcp	2020/11/23 09:22:12	2020/11/23 09:22:12	192.168.105.2	48778	192.168.105.5	1344	352		6
+ tcp	2020/11/23 09:22:07	2020/11/23 09:22:07	192.168.105.2	48777	192.168.105.5	1344	352		6
+ tcp	2020/11/23 09:22:02	2020/11/23 09:22:02	192.168.105.2	48776	192.168.105.5	1344	406		7
+ tcp	2020/11/23 09:21:57	2020/11/23 09:21:57	192.168.105.2	48775	192.168.105.5	1344	352		6
+ tcp	2020/11/23 09:21:52	2020/11/23 09:21:52	192.168.105.2	48774	192.168.105.5	1344	352		6

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided “as is”. Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness or performance

7. Scroll down to get ICAP payload:



```
REQMOD icap://localhost/echo ICAP/1.0
Host: icap-server.net
From: SSLiDemo@Radware.com
User-Agent: ICAP-client-XYZ
X-Client-IP: 192.168.200.1
Encapsulated: req-hdr=0, null-body=1042

GET /.asset/2.248.1/js/chunks/50-a391a1833271da5ccfb6.min.js HTTP/1.1
Host: www.cnn.com
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.198 Safari/537.36
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://www.cnn.com/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: countryCode=US; stateCode=NJ; geoData=newark|NJ|07104|US|NA|-500|broadband|40.770|-74.170;
FastAB=0=5683,1=6830,2=1551,3=2329,4=6803,5=0612,6=1098,7=8753,8=1165,9=1434; psmRetryExternalIds=false;
psmMetaData=%7B%22appId%22%3A%225e9f25a81c9d440000a83808%22%2C%22brand%22%3A%22CNN%22%2C%22environment%22%3A%22PROD%22%2C%22domain%
22%3A%22.cnn.com%22%2C%22location%22%3A%22US%22%7D; usprivacy=1YNN; OptanonControl=ccc=US&otvers=&reg=ccpa&pctm=0&vers=3.0.5;
WMUKID=%7B%22id%22%3A%223f9c5767-64e4-4c0f-9c92-76ae755065be%22%2C%22version%22%3A0.1%2C%22timestamp%22%3A%222020-11-
23T14%3A13%3A21.362Z%22%7D

ICAP/1.0 200 OK
Server: C-ICAP/0.3.5
Connection: keep-alive
ISTag: CI0001-XXXXXXXXX
Encapsulated: req-hdr=0, null-body=1112

GET /.asset/2.248.1/js/chunks/50-a391a1833271da5ccfb6.min.js HTTP/1.1
Host: www.cnn.com
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.198 Safari/537.36
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://www.cnn.com/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: countryCode=US; stateCode=NJ; geoData=newark|NJ|07104|US|NA|-500|broadband|40.770|-74.170;
FastAB=0=5683,1=6830,2=1551,3=2329,4=6803,5=0612,6=1098,7=8753,8=1165,9=1434; psmRetryExternalIds=false;
psmMetaData=%7B%22appId%22%3A%225e9f25a81c9d440000a83808%22%2C%22brand%22%3A%22CNN%22%2C%22environment%22%3A%22PROD
22%3A%22.cnn.com%22%2C%22location%22%3A%22US%22%7D; usprivacy=1YNN; OptanonControl=ccc=US&otvers=&reg=ccpa&pctm=0&vers=3.0.5;
WMUKID=%7B%22id%22%3A%223f9c5767-64e4-4c0f-9c92-76ae755065be%22%2C%22version%22%3A0.1%2C%22timestamp%22%3A%222020-11-
```

8. To inspect the actual traffic flow using packet capture refer to: Appendix C – Running packet capture

2. Scenario 2 – Specific Host Bypass

In this scenario we will demonstrate bypassing SSL inspection based on specific host.

The steps in the scenario include:

1. Browse to www.bbc.com
2. Show that we perform SSL inspection.
3. Enable bypass filter for www.bbc.com
4. Browse again to www.bbc.com
5. Show that we bypass the SSL inspection.
6. Browse to another site.
7. Show that it still gets inspected.

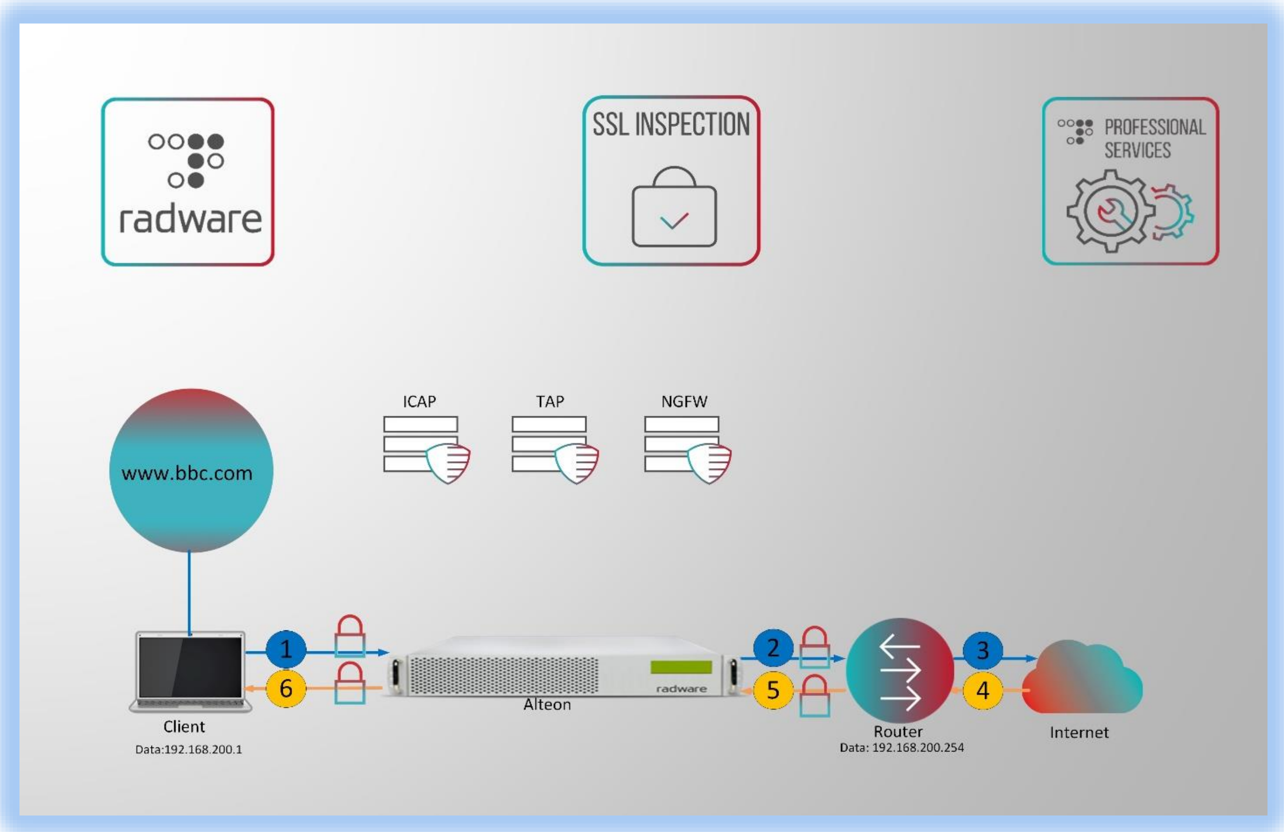
Note:

In order to view the Alteon configuration refer to Appendix F: Scenario 2 configuration
Please Open SSL Inspection analytics using Appendix I: Vision SSL Inspection Analytics

Scenario 2 – Diagram and Traffic Flow

The diagram below details the entire flow of the **bypass** traffic (when bypass filter is enabled):

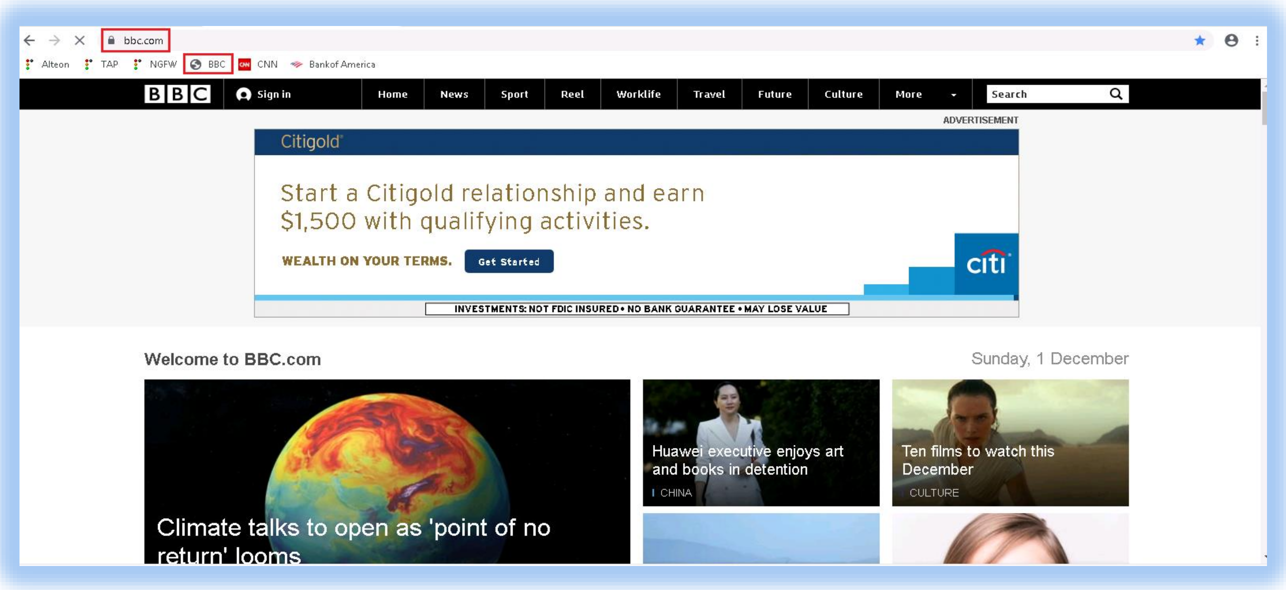
1. The client browses to www.bbc.com.



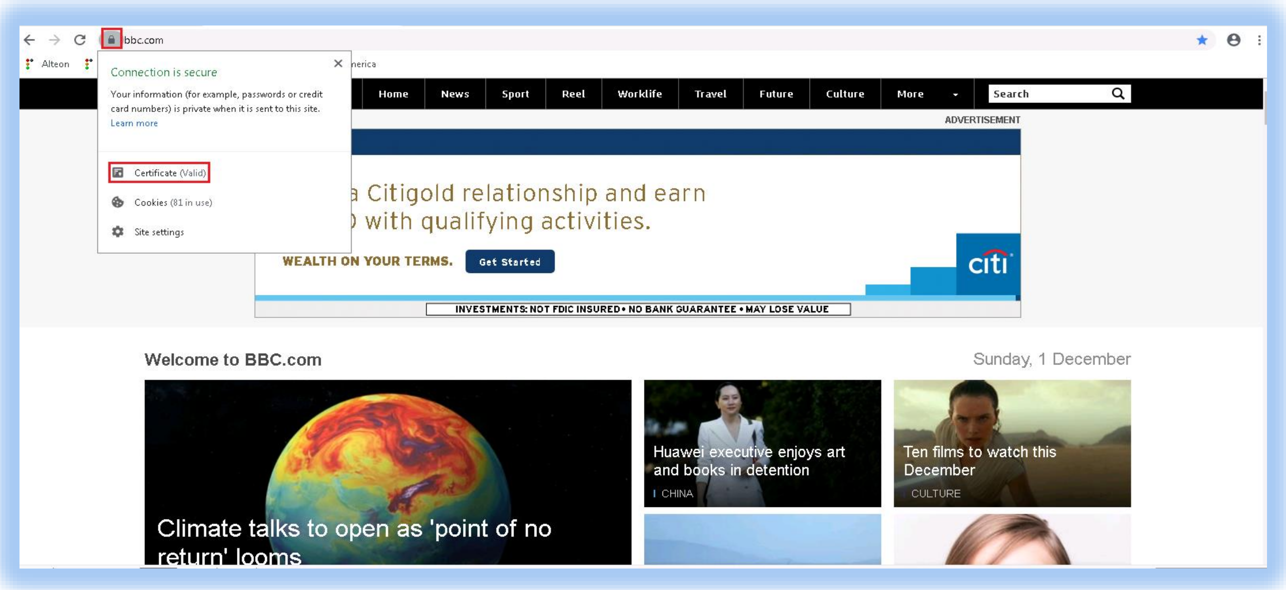
2. Based on the **host name** the Alteon bypasses the SSL Inspection.
3. The Router performs NAT and forwards the request to the internet.
4. The Website sends the response to the router.
5. The Router sends the response to the Alteon.
6. The Alteon sends the response to the client.

Running Scenario 2

1. Open Chrome browser and click on **BBC** bookmark:


bbc.com
Alteon
TAP
NGFW
BBC
CNN
Bank of America
BBC
Sign in
Home
News
Sport
Reel
Worklife
Travel
Future
Culture
More
Search
ADVERTISEMENT
Citigold
Start a Citigold relationship and earn $1,500 with qualifying activities.
WEALTH ON YOUR TERMS.
Get Started
citi
INVESTMENTS: NOT FDIC INSURED • NO BANK GUARANTEE • MAY LOSE VALUE
Welcome to BBC.com
Sunday, 1 December
Climate talks to open as 'point of no return' looms
Huawei executive enjoys art and books in detention
CHINA
Ten films to watch this December
CULTURE

2. Click on the **Lock Button** and then **Certificate** to verify the certificate issuer:


Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

Certificate (Valid)

Cookies (81 in use)

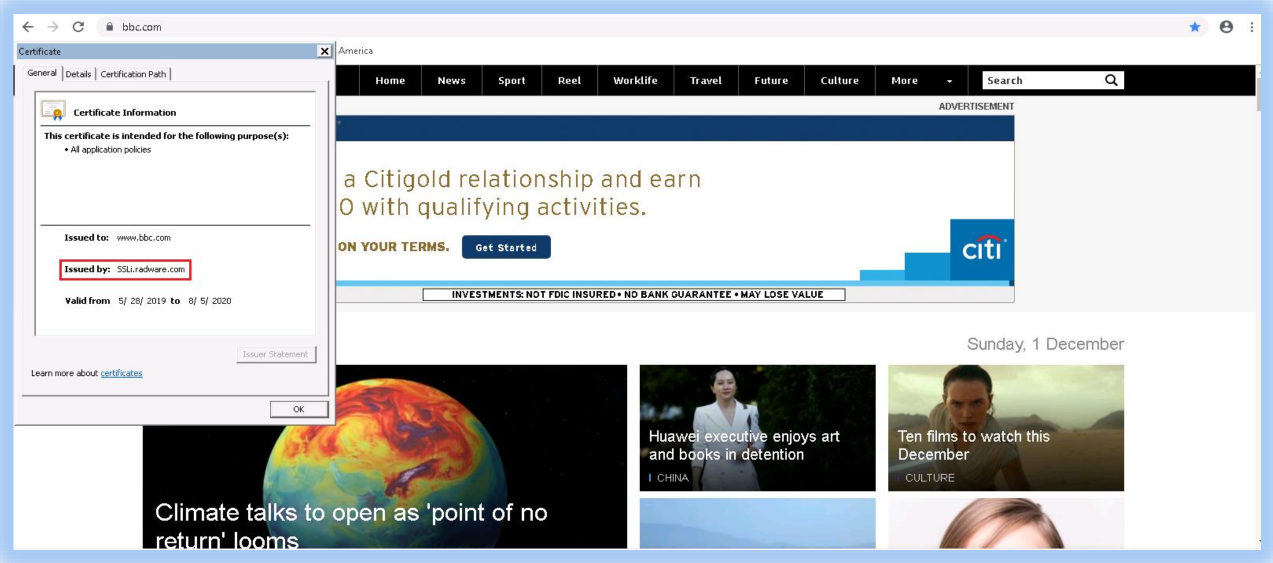
Site settings

bbc.com
Alteon
Home
News
Sport
Reel
Worklife
Travel
Future
Culture
More
Search
ADVERTISEMENT
WEALTH ON YOUR TERMS.
Get Started
citi
INVESTMENTS: NOT FDIC INSURED • NO BANK GUARANTEE • MAY LOSE VALUE
Welcome to BBC.com
Sunday, 1 December
Climate talks to open as 'point of no return' looms
Huawei executive enjoys art and books in detention
CHINA
Ten films to watch this December
CULTURE

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided “as is”. Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness or performance

3. We can see that the certificate was issued by the Alteon, meaning the traffic was forwarded to security devices for inspection and re-encrypted successfully:



Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):
- All application policies

Issued to: www.bbc.com

Issued by: SSLi.radware.com

Valid from 5/ 28/ 2019 to 8/ 5/ 2020

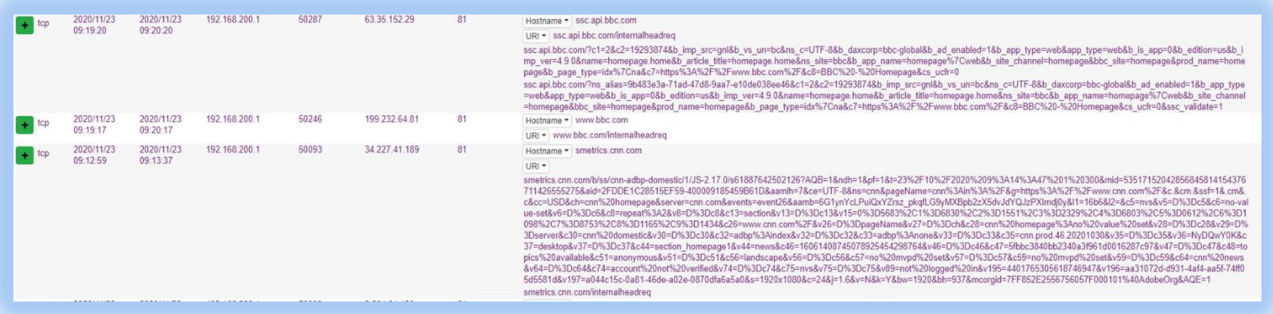
Issuer Statement

Learn more about certificates

OK

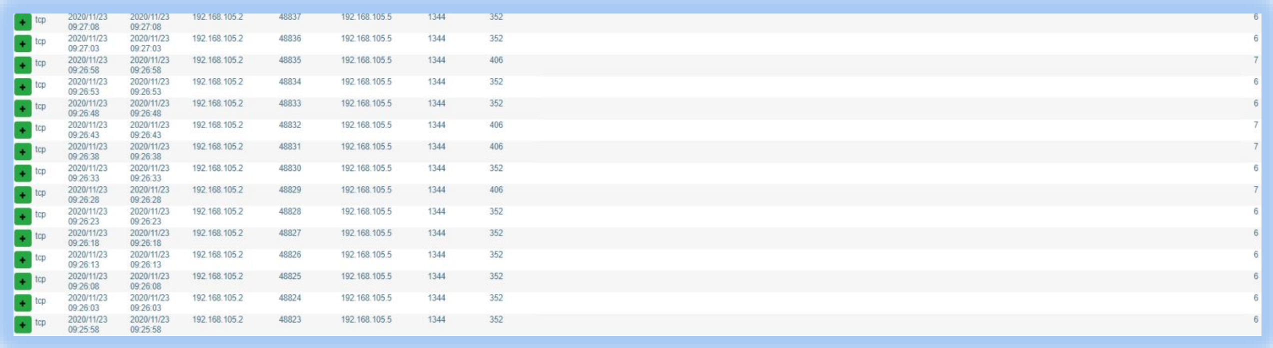
bbc.com
America
Home
News
Sport
Reel
Worklife
Travel
Future
Culture
More
Search
ADVERTISEMENT
a Citigold relationship and earn
0 with qualifying activities.
ON YOUR TERMS.
Get Started
citi
INVESTMENTS: NOT FDIC INSURED • NO BANK GUARANTEE • MAY LOSE VALUE
Sunday, 1 December
Climate talks to open as 'point of no return' looms
Huawei executive enjoys art and books in detention
CHINA
Ten films to watch this December
CULTURE

4. Browse to "TAP" bookmark in order to watch traffic reaching the "TAP" device:



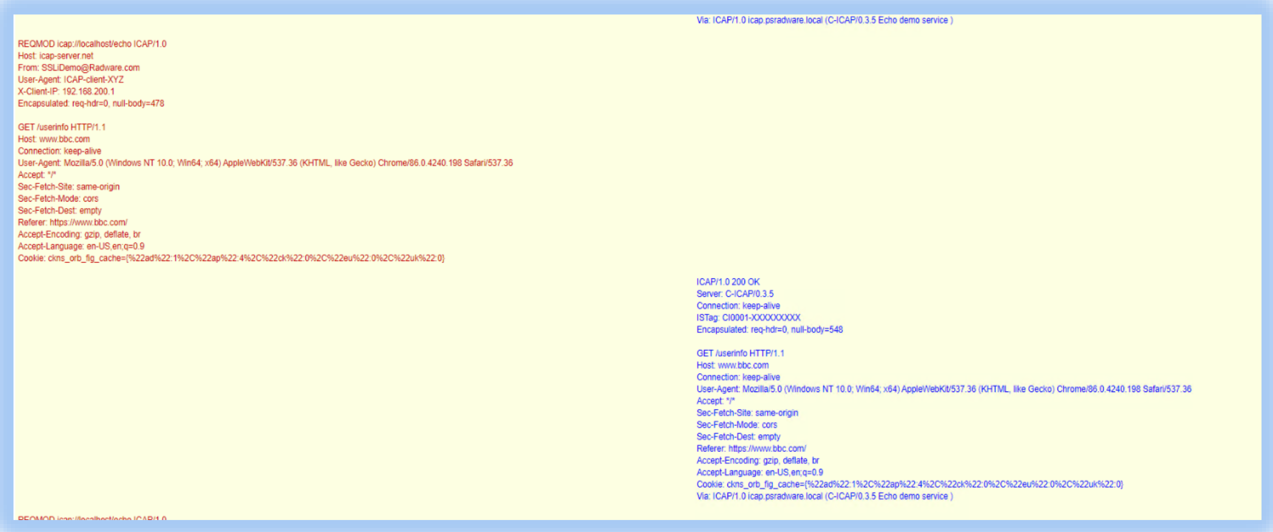
+ tcp	2020/11/23 09:19:20	2020/11/23 09:20:20	192.168.200.1	50287	63.35.152.29	81	Hostname ▾ ssc.api.bbc.com URI ▾ ssc.api.bbc.com/internalheadreq ssc.api.bbc.com/?c1=2&c2=19293874&b_imp_src=gnl&b_vs_un=bc&ns_c=UTF-8&b_daxcorp=bbc-global&b_ad_enabled=1&b_app_type=web&app_type=web&b_is_app=0&b_edition=us&b_imp_ver=4.9.0&name=homepage.home&b_article_title=homepage.home&ns_site=bbc&b_app_name=homepage%7Cweb&b_site_channel=homepage&bbc_site=homepage&prod_name=homepage&b_page_type=idx%7Cna&c7=https%3A%2F%2Fwww.bbc.com%2F&c8=BBC%20-%20Homepage&cs_ucfr=0 ssc.api.bbc.com/?ns_alias=9b483e3a-71ad-47d8-9aa7-e10de038ee46&c1=2&c2=19293874&b_imp_src=gnl&b_vs_un=bc&ns_c=UTF-8&b_daxcorp=bbc-global&b_ad_enabled=1&b_app_type=web&app_type=web&b_is_app=0&b_edition=us&b_imp_ver=4.9.0&name=homepage.home&b_article_title=homepage.home&ns_site=bbc&b_app_name=homepage%7Cweb&b_site_channel=homepage&bbc_site=homepage&prod_name=homepage&b_page_type=idx%7Cna&c7=https%3A%2F%2Fwww.bbc.com%2F&c8=BBC%20-%20Homepage&cs_ucfr=0&ssc_validate=1
+ tcp	2020/11/23 09:19:17	2020/11/23 09:20:17	192.168.200.1	50246	199.232.64.81	81	Hostname ▾ www.bbc.com URI ▾ www.bbc.com/internalheadreq
+ tcp	2020/11/23 09:12:59	2020/11/23 09:13:37	192.168.200.1	50093	34.227.41.189	81	Hostname ▾ smetrics.cnn.com URI ▾ smetrics.cnn.com/b/ss/cnn-adbp-domestic/1/JS-2.17.0/s61887642502126?AQB=1&ndh=1&pf=1&t=23%2F10%2F2020%209%3A14%3A47%201%20300&mid=53517152042856845814154376711426555275&aid=2FDDE1C28515EF59-40000918545 9B61D&aamlh=7&ce=UTF-8&ns=cnn&pageName=cnn%3Ain%3A%2F&g=https%3A%2F%2Fwww.cnn.com%2F&c.&cm.&ssf=1&.cm&.c&cc=USD&ch=cnn%20homepage&server=cnn.com&events=event26&aamb=6G1ynYcLPuiQxYZrsz_pkqfLG9yMXBpb2zX5dvJdYQJzPXImdj0y&l1=16b6&l2=&c5=nvs&v5=D%3Dc5&c6=no-value-set&v6=D%3Dc6&c8=repeat%3A2&v8=D%3Dc8&c13=section&v13=D%3Dc13&v15=0%3D5683%2C1%3D6830%2C2%3D1551%2C3%3D2329%2C4%3D6803%2C5%3D0612%2C6%3D1098%2C7%3D8753%2C8%3D1165%2C9%3D1434&c26=www.cnn.com%2F&v26=D%3DpageName&v27=D%3Dch&c28=cnn%20homepage%3Ano%20value%20set&v28=D%3Dc28&v29=D%3Dserver&c30=cnn%20domestic&v30=D%3Dc30&c32=adbp%3Aindex&v32=D%3Dc32&c33=adbp%3Anone&v33=D%3Dc33&c35=cnn.prod.46.20201030&v35=D%3Dc35&v36=NyDQwY0K&c37=desktop&v37=D%3Dc37&c44=section_homepage1&v44=news&c46=1606140874507892545429 8764&v46=D%3Dc46&c47=5fbbc3840bb2340a3f961d0016287c97&v47=D%3Dc47&c48=topics%20available&c51=anonymous&v51=D%3Dc51&c56=landscape&v56=D%3Dc56&c57=no%20mvpd%20set&v57=D%3Dc57&c59=no%20mvpd%20set&v59=D%3Dc59&c64=cnn%20news&v64=D%3Dc64&c74=account%20not%20verified&v74=D%3Dc74&c75=nvs&v75=D%3Dc75&v89=not%20logged%20in&v195=4401765305618746947&v196=aa31072d-d931-4af4-aa5f-74ff05d5581d&v197=a044c15c-0a81-46de-a02e-0870dfa6a5a0&s=1920x1080&c=24&j=1.6&v=N&k=Y&bw=1920&bh=937&mcorgid=7FF852E2556756057F000101%40AdobeOrg&AQE=1 smetrics.cnn.com/internalheadreq

5. Browse to "ICAP" bookmark in order to watch traffic reaching the ICAP device and click the "+" button:



+	tcp	2020/11/23 09:27:08	2020/11/23 09:27:08	192.168.105.2	48837	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:27:03	2020/11/23 09:27:03	192.168.105.2	48836	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:26:58	2020/11/23 09:26:58	192.168.105.2	48835	192.168.105.5	1344	406	7
+	tcp	2020/11/23 09:26:53	2020/11/23 09:26:53	192.168.105.2	48834	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:26:48	2020/11/23 09:26:48	192.168.105.2	48833	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:26:43	2020/11/23 09:26:43	192.168.105.2	48832	192.168.105.5	1344	406	7
+	tcp	2020/11/23 09:26:38	2020/11/23 09:26:38	192.168.105.2	48831	192.168.105.5	1344	406	7
+	tcp	2020/11/23 09:26:33	2020/11/23 09:26:33	192.168.105.2	48830	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:26:28	2020/11/23 09:26:28	192.168.105.2	48829	192.168.105.5	1344	406	7
+	tcp	2020/11/23 09:26:23	2020/11/23 09:26:23	192.168.105.2	48828	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:26:18	2020/11/23 09:26:18	192.168.105.2	48827	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:26:13	2020/11/23 09:26:13	192.168.105.2	48826	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:26:08	2020/11/23 09:26:08	192.168.105.2	48825	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:26:03	2020/11/23 09:26:03	192.168.105.2	48824	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:25:58	2020/11/23 09:25:58	192.168.105.2	48823	192.168.105.5	1344	352	6

6. Scroll down to get ICAP payload:

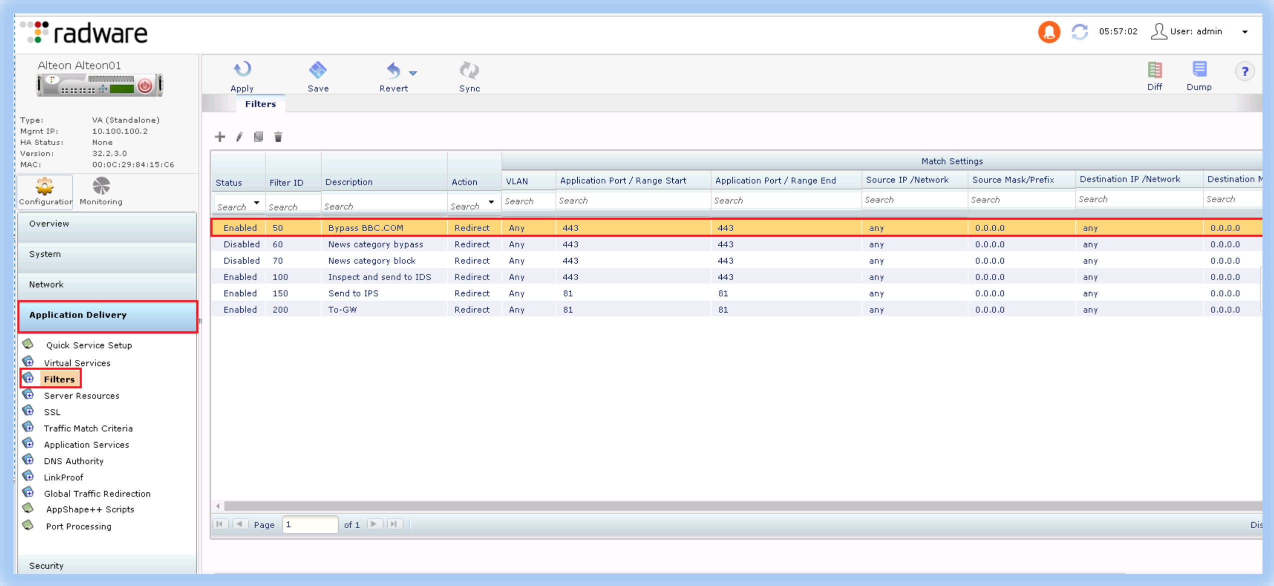


```
                                                  Via: ICAP/1.0 icap.psradware.local (C-ICAP/0.3.5 Echo demo service )

REQMOD icap://localhost/echo ICAP/1.0
Host: icap-server.net
From: SSLiDemo@Radware.com
User-Agent: ICAP-client-XYZ
X-Client-IP: 192.168.200.1
Encapsulated: req-hdr=0, null-body=478

GET /userinfo HTTP/1.1
Host: www.bbc.com
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.198 Safari/537.36
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://www.bbc.com/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: ckns_orb_fig_cache={%22ad%22:1%2C%22ap%22:4%2C%22ck%22:0%2C%22eu%22:0%2C%22uk%22:0}

                                                  ICAP/1.0 200 OK
                                                  Server: C-ICAP/0.3.5
                                                  Connection: keep-alive
                                                  ISTag: CI0001-XXXXXXXXX
                                                  Encapsulated: req-hdr=0, null-body=548

                                                  GET /userinfo HTTP/1.1
                                                  Host: www.bbc.com
                                                  Connection: keep-alive
                                                  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.198 Safari/537.36
                                                  Accept: */*
                                                  Sec-Fetch-Site: same-origin
                                                  Sec-Fetch-Mode: cors
                                                  Sec-Fetch-Dest: empty
                                                  Referer: https://www.bbc.com/
                                                  Accept-Encoding: gzip, deflate, br
                                                  Accept-Language: en-US,en;q=0.9
                                                  Cookie: ckns_orb_fig_cache={%22ad%22:1%2C%22ap%22:4%2C%22ck%22:0%2C%22eu%22:0%2C%22uk%22:0}
                                                  Via: ICAP/1.0 icap.psradware.local (C-ICAP/0.3.5 Echo demo service )
REQMOD icap://localhost/echo ICAP/1.0
```

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided “as is”. Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness or performance

7. Enable the **bypass** filter for www.bbc.com:
   - Login to the Alteon
   - Navigate to **Application Delivery → Filters**
   - Enable **filter 50**

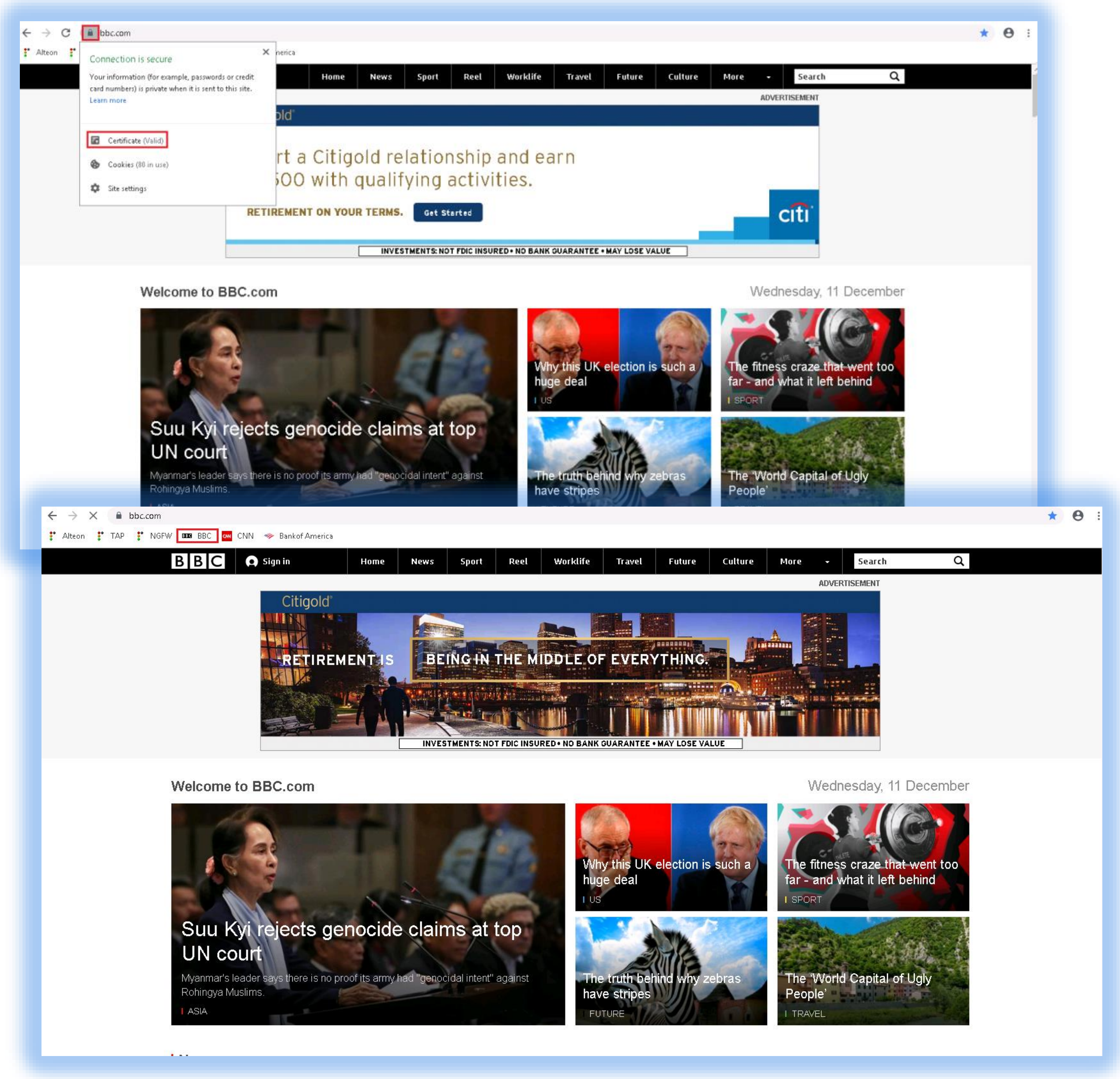


Type:	VA (Standalone)
Mgmt IP:	10.100.100.2
HA Status:	None
Version:	32.2.3.0
MAC:	00:0C:29:84:15:C6

				Match Settings						
Status	Filter ID	Description	Action	VLAN	Application Port / Range Start	Application Port / Range End	Source IP /Network	Source Mask/Prefix	Destination IP /Network	Destination M
Enabled	50	Bypass BBC.COM	Redirect	Any	443	443	any	0.0.0.0	any	0.0.0.0
Disabled	60	News category bypass	Redirect	Any	443	443	any	0.0.0.0	any	0.0.0.0
Disabled	70	News category block	Redirect	Any	443	443	any	0.0.0.0	any	0.0.0.0
Enabled	100	Inspect and send to IDS	Redirect	Any	443	443	any	0.0.0.0	any	0.0.0.0
Enabled	150	Send to IPS	Redirect	Any	81	81	any	0.0.0.0	any	0.0.0.0
Enabled	200	To-GW	Redirect	Any	81	81	any	0.0.0.0	any	0.0.0.0

8. Click on **BBC** bookmark:

9. Click on the **Lock Button** and then **Certificate** button to verify the certificate issuer:



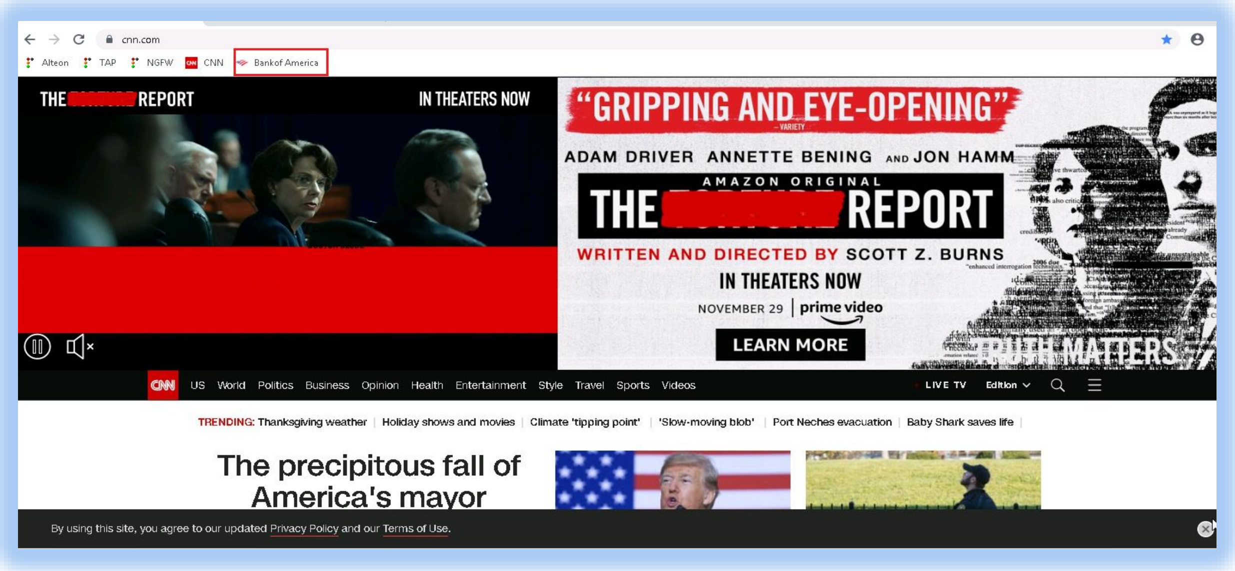
Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

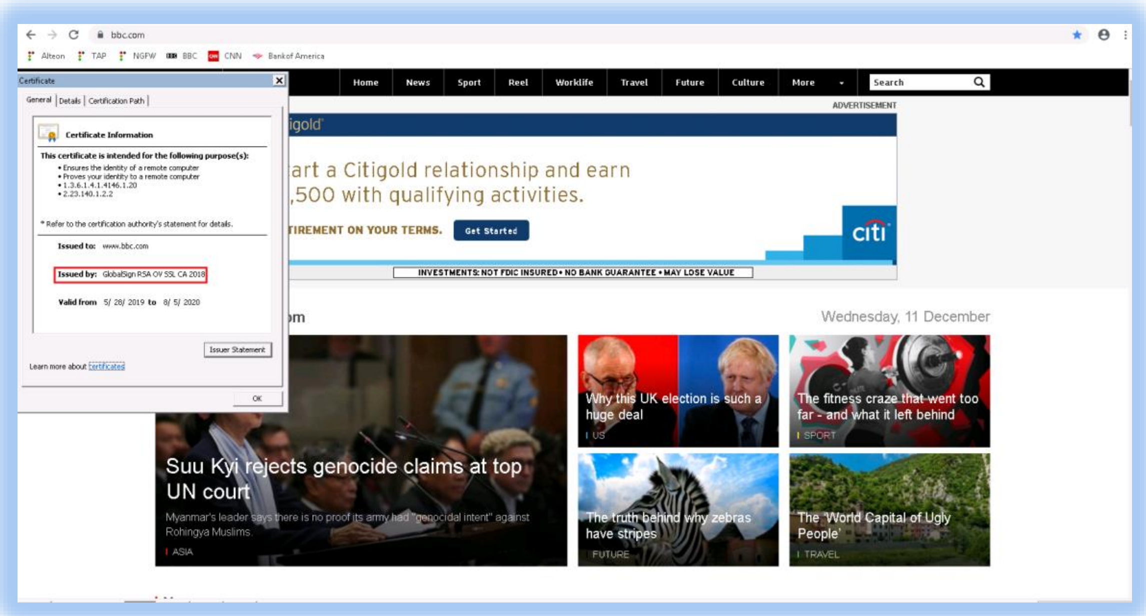
bbc.com
Certificate (Valid)
Cookies (88 in use)
Site settings
Alteon
TAP
NGFW
BBC
CNN
Bank of America
Sign in
Home
News
Sport
Reel
Worklife
Travel
Future
Culture
More
Search
ADVERTISEMENT
Citigold
RETIREMENT IS BEING IN THE MIDDLE OF EVERYTHING.
RETIREMENT ON YOUR TERMS.
Get Started
INVESTMENTS: NOT FDIC INSURED • NO BANK GUARANTEE • MAY LOSE VALUE
Welcome to BBC.com
Wednesday, 11 December
Suu Kyi rejects genocide claims at top UN court
Myanmar's leader says there is no proof its army had "genocidal intent" against Rohingya Muslims.
ASIA
Why this UK election is such a huge deal
US
The fitness craze that went too far - and what it left behind
SPORT
The truth behind why zebras have stripes
FUTURE
The 'World Capital of Ugly People'
TRAVEL

10. We can see that the **certificate wasn't issued by Alteon** which means the **request was served directly from the web server**, effectively **bypassing the SSL inspection**.

11. Click on **Bank of America** bookmark:


cnn.com
Alteon
TAP
NGFW
CNN
Bankof America
THE [redacted] REPORT
IN THEATERS NOW
"GRIPPING AND EYE-OPENING"
VARIETY
ADAM DRIVER ANNETTE BENING AND JON HAMM
AMAZON ORIGINAL
THE [redacted] REPORT
WRITTEN AND DIRECTED BY SCOTT Z. BURNS
IN THEATERS NOW
NOVEMBER 29 | prime video
LEARN MORE
TRUTH MATTERS
US World Politics Business Opinion Health Entertainment Style Travel Sports Videos
LIVE TV
Edition
TRENDING: Thanksgiving weather | Holiday shows and movies | Climate 'tipping point' | 'Slow-moving blob' | Port Neches evacuation | Baby Shark saves life
The precipitous fall of America's mayor

By using this site, you agree to our updated Privacy Policy and our Terms of Use.


bbc.com
Alteon
TAP
NGFW
BBC
CNN
Bankof America
Home News Sport Reel Worklife Travel Future Culture More
Search
ADVERTISEMENT
igold
art a Citigold relationship and earn
,500 with qualifying activities.
TIREMENT ON YOUR TERMS.
Get Started
citi
INVESTMENTS: NOT FDIC INSURED • NO BANK GUARANTEE • MAY LOSE VALUE
Wednesday, 11 December
Suu Kyi rejects genocide claims at top UN court
Myanmar's leader says there is no proof its army had "genocidal intent" against Rohingya Muslims.
ASIA
Why this UK election is such a huge deal
US
The fitness craze that went too far - and what it left behind
SPORT
The truth behind why zebras have stripes
FUTURE
The 'World Capital of Ugly People'
TRAVEL

Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- 1.3.6.1.4.1.4146.1.20
- 2.23.140.1.2.2

* Refer to the certification authority's statement for details.

Issued to: www.bbc.com

Issued by: GlobalSign RSA OV SSL CA 2018

Valid from 5/ 28/ 2019 to 8/ 5/ 2020

Issuer Statement

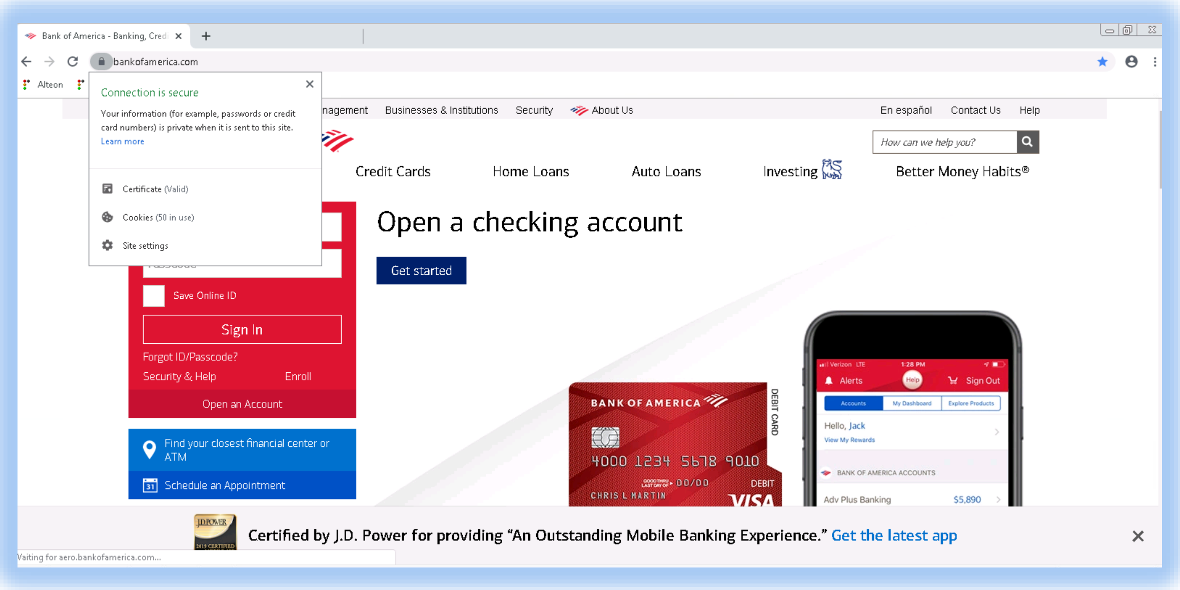
Learn more about certificates

OK

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided "as is". Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness or performance

12. Click on the **Lock Button** and then **Certificate** to verify the certificate issuer:



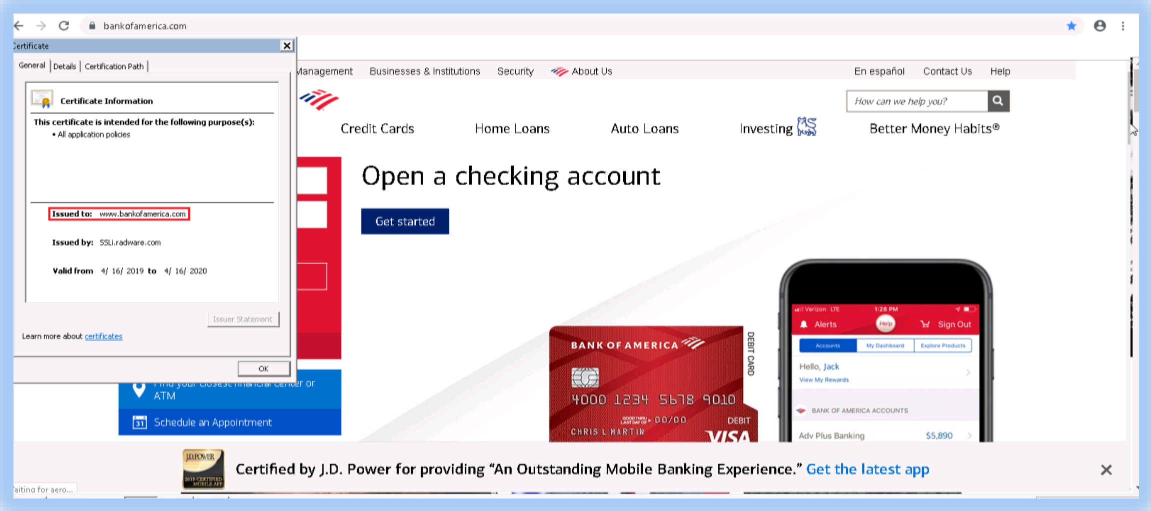
Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site.

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided “as is”. Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness or performance

13. We can see that the **certificate was issued by the Alteon**, meaning the **traffic was forwarded to security devices for inspection** and re-encrypted successfully:



Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):
- All application policies

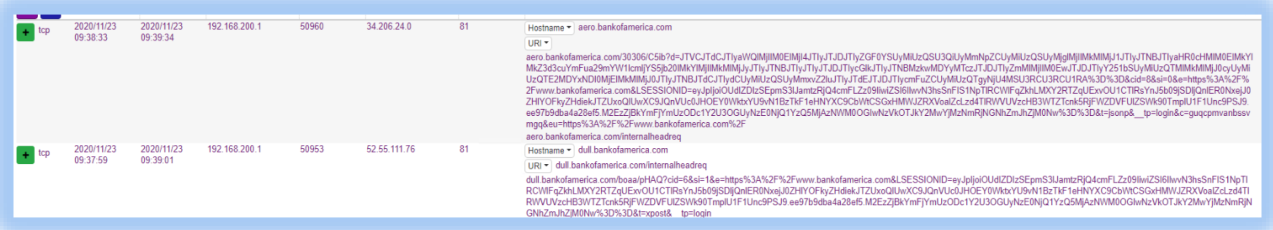
Issued to: www.bankofamerica.com

Issued by: SSLi.radware.com

Valid from 4/ 16/ 2019 to 4/ 16/ 2020

Learn more about certificates

14. Browse to "TAP" bookmark in order to watch traffic reaching the "TAP" device:

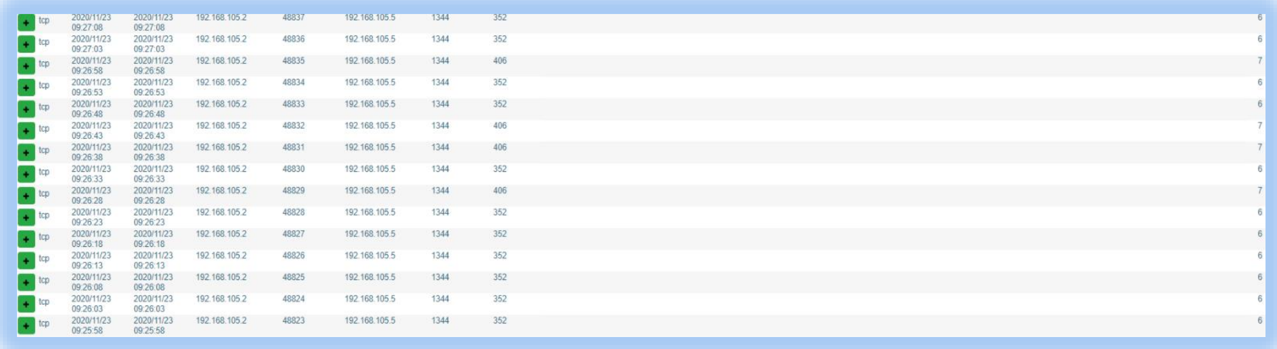


+	tcp	2020/11/23 09:38:33	2020/11/23 09:39:34	192.168.200.1	50960	34.206.24.0	81	Hostname ▾ aero.bankofamerica.com URI ▾ aero.bankofamerica.com/30306/C5ib?d=JTVCJTdCJTIyaWQlMjIlM0ElMjI4JTIyJTJDJTIyZGF0YSUyMiUzQSU3QiUyMmNpZCUyMiUzQSUyMjglMjIlMkMlMjJ1JTIyJTNBJTIyaHR0cHMlM0ElMkYlMkZ3d3cuYmFua29mYW1lcmljYS5jb20lMkYlMjIlMkMlMjJyJTIyJTNBJTIyJTIyJTJDJTIycGlkJTIyJTNBMzkwMDYyMTczJTJDJTIyZmMlMjIlM0EwJTJDJTIyY251bSUyMiUzQTMlMkMlMjJ0cyUyMiUzQTE2MDYxNDI0MjElMkMlMjJ0JTIyJTNBJTdCJTIydCUyMiUzQSUyMmxvZ2luJTIyJTdEJTJDJTIycmFuZCUyMiUzQTgyNjU4MSU3RCU3RCU1RA%3D%3D&cid=8&si=0&e=https%3A%2F%2Fwww.bankofamerica.com&LSESSIONID=eyJpljoiOUdIZDIzSEpmS3lJamtzRjQ4cmFLZz09IiwiZSI6IlwvN3hsSnFIS1NpTlRCWlFqZkhLMXY2RTZqUExvOU1CTlRsYnJ5b09jSDljQnlER0NxejJ0ZHlYOFkyZHdiekJTZUxoQlUwXC9JQnVUc0JHOEY0WktxYU9vN1BzTkF1eHNYXC9CbWtCSGxHMWJZRXVoalZcLzd4TlRWVUVzcHB3WTZTcnk5RjFWZDVFUlZSWk90TmplU1F1Unc9PSJ9.ee97b9dba4a28ef5.M2EzZjBkYmFjYmUzODc1Y2U3OGUyNzE0NjQ1YzQ5MjAzNWM0OGIwNzVkOTJkY2MwYjMzNmRjNGNhZmJhZjM0Nw%3D%3D&t=jsonp&__tp=login&c=guqcpmvanbssvmgq&eu=https%3A%2F%2Fwww.bankofamerica.com%2F aero.bankofamerica.com/internalheadreq
+	tcp	2020/11/23 09:37:59	2020/11/23 09:39:01	192.168.200.1	50953	52.55.111.76	81	Hostname ▾ dull.bankofamerica.com URI ▾ dull.bankofamerica.com/internalheadreq dull.bankofamerica.com/boaa/pHAQ?cid=6&si=1&e=https%3A%2F%2Fwww.bankofamerica.com&LSESSIONID=eyJpljoiOUdIZDIzSEpmS3lJamtzRjQ4cmFLZz09IiwiZSI6IlwvN3hsSnFIS1NpTlRCWlFqZkhLMXY2RTZqUExvOU1CTlRsYnJ5b09jSDljQnlER0NxejJ0ZHlYOFkyZHdiekJTZUxoQlUwXC9JQnVUc0JHOEY0WktxYU9vN1BzTkF1eHNYXC9CbWtCSGxHMWJZRXVoalZcLzd4TlRWVUVzcHB3WTZTcnk5RjFWZDVFUlZSWk90TmplU1F1Unc9PSJ9.ee97b9dba4a28ef5.M2EzZjBkYmFjYmUzODc1Y2U3OGUyNzE0NjQ1YzQ5MjAzNWM0OGIwNzVkOTJkY2MwYjMzNmRjNGNhZmJhZjM0Nw%3D%3D&t=xpost&__tp=login

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

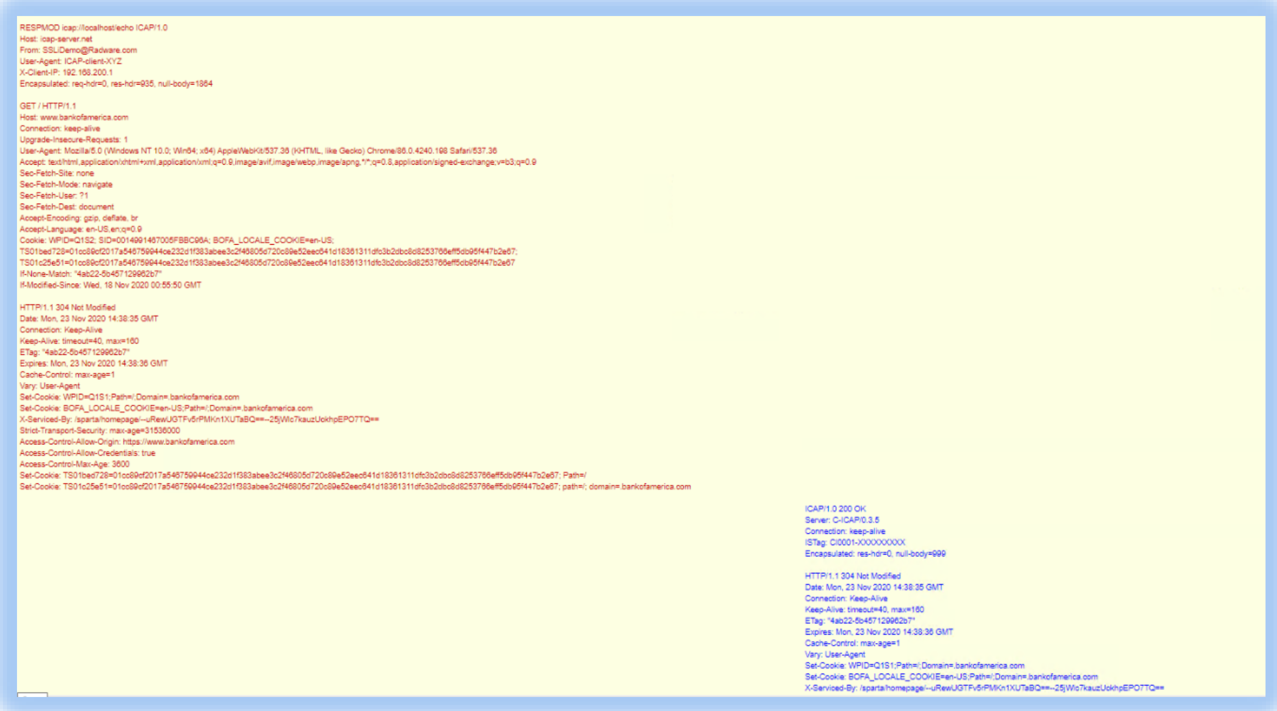
All information provided in the Demo lab and documentation is provided "as is". Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness or performance

15. Browse to "ICAP" bookmark in order to watch traffic reaching the ICAP device and click the "+" button:



+	tcp	2020/11/23 09:27:08	2020/11/23 09:27:08	192.168.105.2	48837	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:27:03	2020/11/23 09:27:03	192.168.105.2	48836	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:26:58	2020/11/23 09:26:58	192.168.105.2	48835	192.168.105.5	1344	406	7
+	tcp	2020/11/23 09:26:53	2020/11/23 09:26:53	192.168.105.2	48834	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:26:48	2020/11/23 09:26:48	192.168.105.2	48833	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:26:43	2020/11/23 09:26:43	192.168.105.2	48832	192.168.105.5	1344	406	7
+	tcp	2020/11/23 09:26:38	2020/11/23 09:26:38	192.168.105.2	48831	192.168.105.5	1344	406	7
+	tcp	2020/11/23 09:26:33	2020/11/23 09:26:33	192.168.105.2	48830	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:26:28	2020/11/23 09:26:28	192.168.105.2	48829	192.168.105.5	1344	406	7
+	tcp	2020/11/23 09:26:23	2020/11/23 09:26:23	192.168.105.2	48828	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:26:18	2020/11/23 09:26:18	192.168.105.2	48827	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:26:13	2020/11/23 09:26:13	192.168.105.2	48826	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:26:08	2020/11/23 09:26:08	192.168.105.2	48825	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:26:03	2020/11/23 09:26:03	192.168.105.2	48824	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:25:58	2020/11/23 09:25:58	192.168.105.2	48823	192.168.105.5	1344	352	6

16. Scroll down to get ICAP payload:



```
RESPMOD icap://localhost/echo ICAP/1.0
Host: icap-server.net
From: SSLiDemo@Radware.com
User-Agent: ICAP-client-XYZ
X-Client-IP: 192.168.200.1
Encapsulated: req-hdr=0, res-hdr=935, null-body=1864

GET / HTTP/1.1
Host: www.bankofamerica.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.198 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: WPID=Q1S2; SID=0014991467005FBBC96A; BOFA_LOCALE_COOKIE=en-US;
TS01bed728=01cc89cf2017a546759944ce232d1f383abee3c2f46805d720c89e52eec641d18361311dfc3b2dbc8d8253766eff5db95f447b2e67;
TS01c25e51=01cc89cf2017a546759944ce232d1f383abee3c2f46805d720c89e52eec641d18361311dfc3b2dbc8d8253766eff5db95f447b2e67
If-None-Match: "4ab22-5b457129962b7"
If-Modified-Since: Wed, 18 Nov 2020 00:55:50 GMT

HTTP/1.1 304 Not Modified
Date: Mon, 23 Nov 2020 14:38:35 GMT
Connection: Keep-Alive
Keep-Alive: timeout=40, max=160
ETag: "4ab22-5b457129962b7"
Expires: Mon, 23 Nov 2020 14:38:36 GMT
Cache-Control: max-age=1
Vary: User-Agent
Set-Cookie: WPID=Q1S1;Path=/;Domain=.bankofamerica.com
Set-Cookie: BOFA_LOCALE_COOKIE=en-US;Path=/;Domain=.bankofamerica.com
X-Serviced-By: /sparta/homepage/--uRewUGTFv5rPMKn1XUTaBQ==--25jWlc7kauzUckhpEPO7TQ==
Strict-Transport-Security: max-age=31536000
Access-Control-Allow-Origin: https://www.bankofamerica.com
Access-Control-Allow-Credentials: true
Access-Control-Max-Age: 3600
Set-Cookie: TS01bed728=01cc89cf2017a546759944ce232d1f383abee3c2f46805d720c89e52eec641d18361311dfc3b2dbc8d8253766eff5db95f447b2e67; Path=/
Set-Cookie: TS01c25e51=01cc89cf2017a546759944ce232d1f383abee3c2f46805d720c89e52eec641d18361311dfc3b2dbc8d8253766eff5db95f447b2e67; path=/; domain=.bankofamerica.com

ICAP/1.0 200 OK
Server: C-ICAP/0.3.5
Connection: keep-alive
ISTag: CI0001-XXXXXXXXX
Encapsulated: res-hdr=0, null-body=999

HTTP/1.1 304 Not Modified
Date: Mon, 23 Nov 2020 14:38:35 GMT
Connection: Keep-Alive
Keep-Alive: timeout=40, max=160
ETag: "4ab22-5b457129962b7"
Expires: Mon, 23 Nov 2020 14:38:36 GMT
Cache-Control: max-age=1
Vary: User-Agent
Set-Cookie: WPID=Q1S1;Path=/;Domain=.bankofamerica.com
Set-Cookie: BOFA_LOCALE_COOKIE=en-US;Path=/;Domain=.bankofamerica.com
X-Serviced-By: /sparta/homepage/--uRewUGTFv5rPMKn1XUTaBQ==--25jWlc7kauzUckhpEPO7TQ==
```

3. Scenario 3 – Category Based Bypass

In this scenario we will demonstrate bypassing SSL inspection based on a category of web sites (NEWS in our example).

The steps in the scenario include:

1. Browse to www.cnn.com
2. Show that we perform SSL inspection.
3. Enable bypass filter for NEWS web category.
4. Browse again to www.cnn.com
5. Show that we bypass the SSL inspection.
6. Browse to another site.
7. Show that it still gets inspected.

Note:

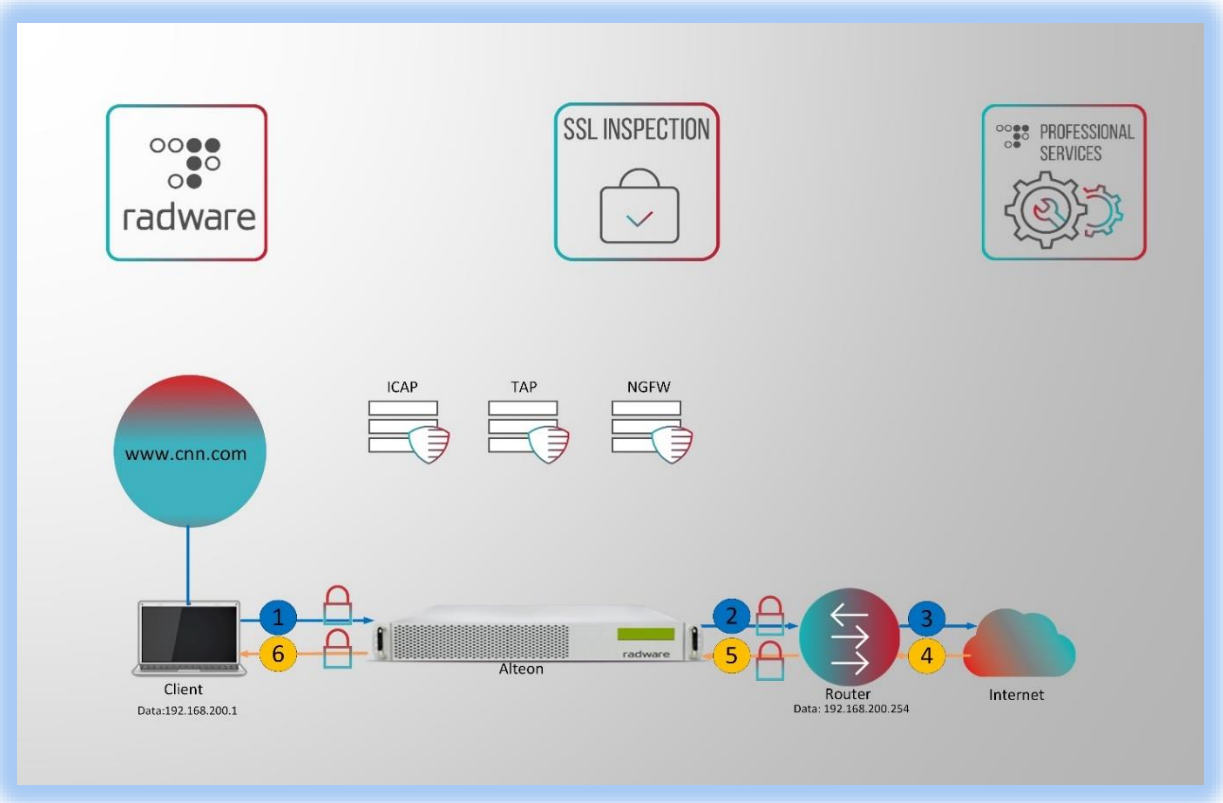
In order to view the Alteon configuration refer to Appendix H: Scenario 3 Configuration
Please Open SSL Inspection analytics using Appendix I: Vision SSL Inspection Analytics

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided “as is”. Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness or performance

Diagram and Traffic Flow

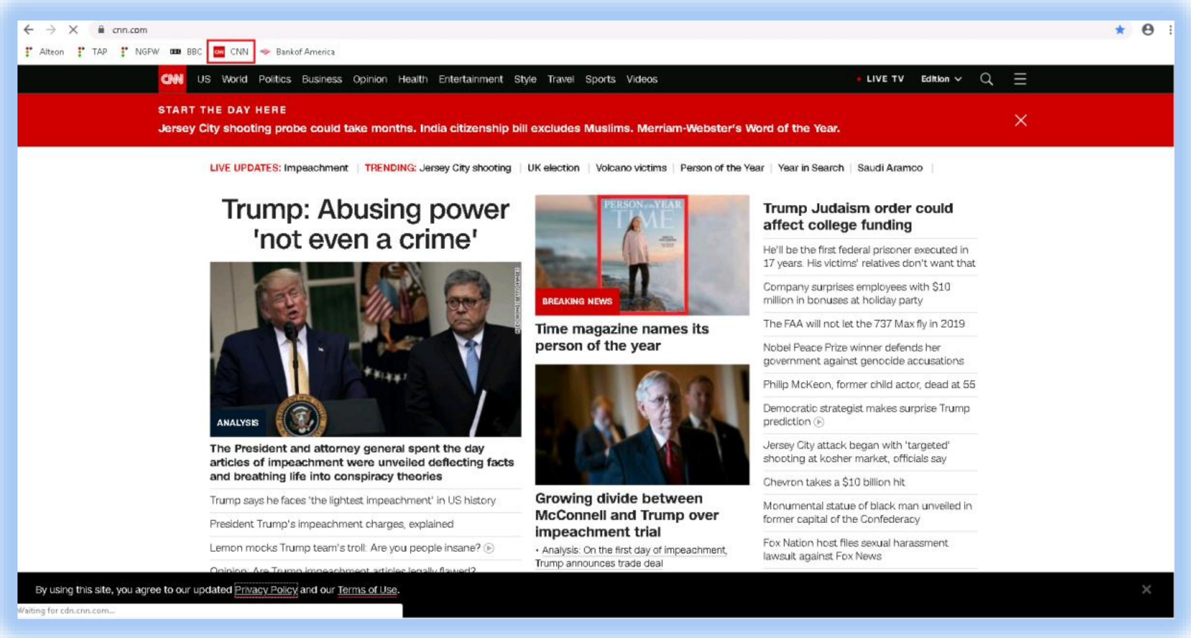
The diagram below details the entire flow of the **bypass** traffic (when bypass filter is enabled):



1. The client browses to www.cnn.com.
2. Based on web category filtering policy the Alteon bypasses the SSL inspection.
3. The Router performs NAT and forwards the request to the internet.
4. The Website sends the response to the router.
5. The Router sends the response to the Alteon.
6. The Alteon sends the response to the client.

Running the Demo Scenario

1. Click on **CNN** bookmark:



START THE DAY HERE

Jersey City shooting probe could take months. India citizenship bill excludes Muslims. Merriam-Webster's Word of the Year.

LIVE UPDATES: Impeachment | TRENDING: Jersey City shooting | UK election | Volcano victims | Person of the Year | Year in Search | Saudi Aramco |

Trump: Abusing power 'not even a crime'

The President and attorney general spent the day articles of impeachment were unveiled deflecting facts and breathing life into conspiracy theories

Trump says he faces 'the lightest impeachment' in US history

President Trump's impeachment charges, explained

Lemon mocks Trump team's troll: Are you people insane?

Opinion: Are Trump impeachment articles legally flawed?

Time magazine names its person of the year

Growing divide between McConnell and Trump over impeachment trial

- Analysis: On the first day of impeachment, Trump announces trade deal

Trump Judaism order could affect college funding

He'll be the first federal prisoner executed in 17 years. His victims' relatives don't want that

Company surprises employees with $10 million in bonuses at holiday party

The FAA will not let the 737 Max fly in 2019

Nobel Peace Prize winner defends her government against genocide accusations

Philip McKeon, former child actor, dead at 55

Democratic strategist makes surprise Trump prediction

Jersey City attack began with 'targeted' shooting at kosher market, officials say

Chevron takes a $10 billion hit

Monumental statue of black man unveiled in former capital of the Confederacy

Fox Nation host files sexual harassment lawsuit against Fox News

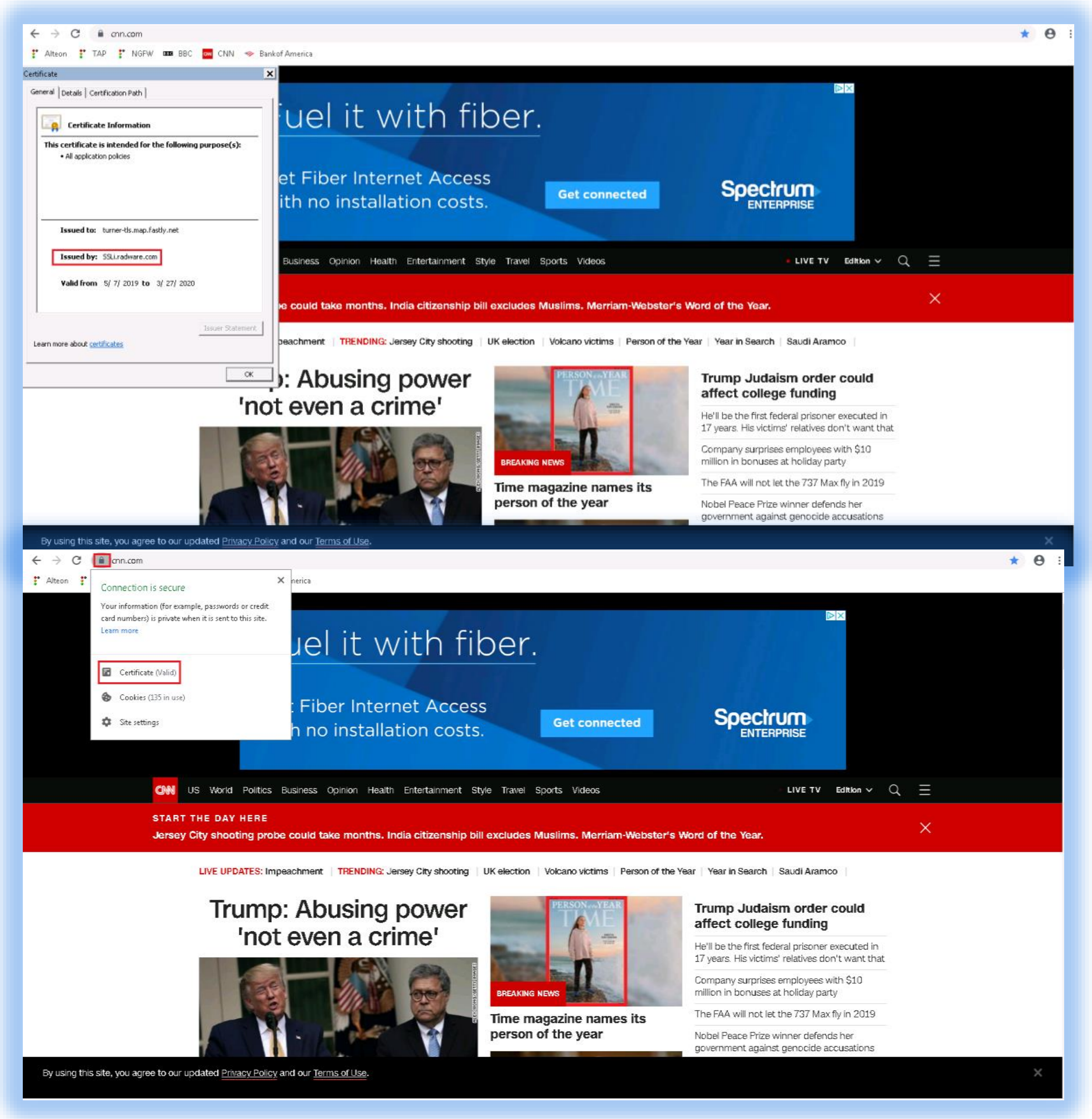
By using this site, you agree to our updated Privacy Policy and our Terms of Use.

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided “as is”. Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness or performance

2. Click on the **Lock Button** and then **Certificate** to verify the certificate issuer:

3. We can see that the certificate was issued by the Alteon, meaning the traffic was forwarded to security devices for inspection and re-encrypted successfully:



Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):
- All application policies

Issued to: turner-tls.map.fastly.net

Issued by: SSLi.radware.com

Valid from 5/ 7/ 2019 to 3/ 27/ 2020

Learn more about certificates

Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site.
Learn more

Certificate (Valid)
Cookies (135 in use)
Site settings

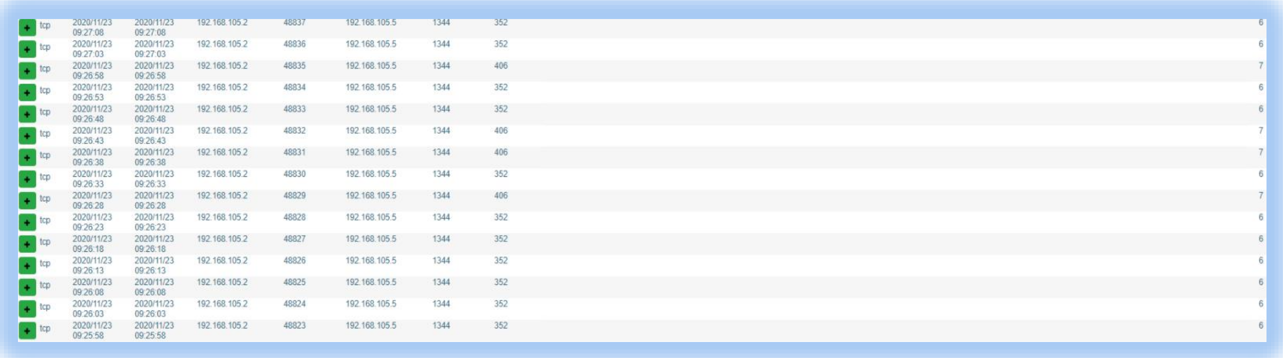
cnn.com
Alteon
TAP
NGFW
BBC
CNN
Bankof America
Issuer Statement
OK
uel it with fiber.
et Fiber Internet Access
ith no installation costs.
Get connected
Spectrum ENTERPRISE
US World Politics Business Opinion Health Entertainment Style Travel Sports Videos
LIVE TV
Edition
START THE DAY HERE
Jersey City shooting probe could take months. India citizenship bill excludes Muslims. Merriam-Webster's Word of the Year.
LIVE UPDATES: Impeachment
TRENDING: Jersey City shooting
UK election
Volcano victims
Person of the Year
Year in Search
Saudi Aramco
Trump: Abusing power 'not even a crime'
BREAKING NEWS
Time magazine names its person of the year
Trump Judaism order could affect college funding
He'll be the first federal prisoner executed in 17 years. His victims' relatives don't want that
Company surprises employees with $10 million in bonuses at holiday party
The FAA will not let the 737 Max fly in 2019
Nobel Peace Prize winner defends her government against genocide accusations
By using this site, you agree to our updated Privacy Policy and our Terms of Use.

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided “as is”. Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness or performance

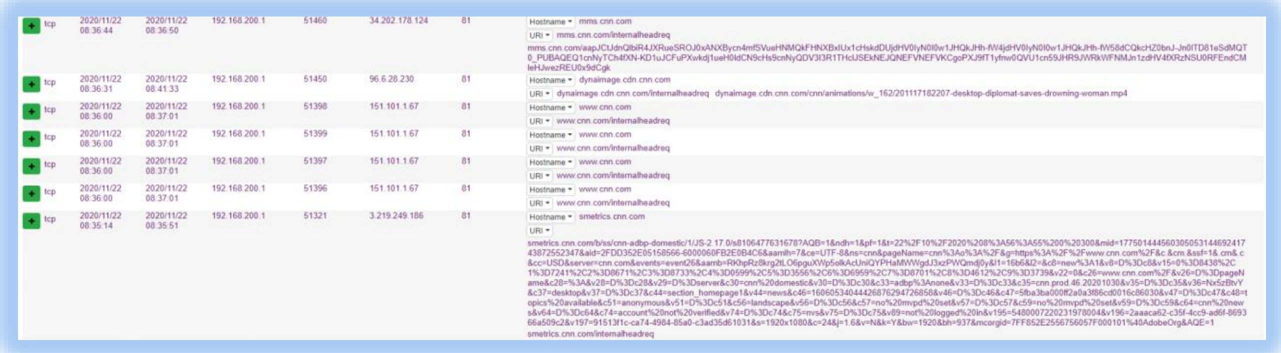
4. Browse to "TAP" bookmark in order to watch traffic reaching the "TAP" device:

5. Browse to "ICAP" bookmark in order to watch traffic reaching the ICAP device and click the "+" button:

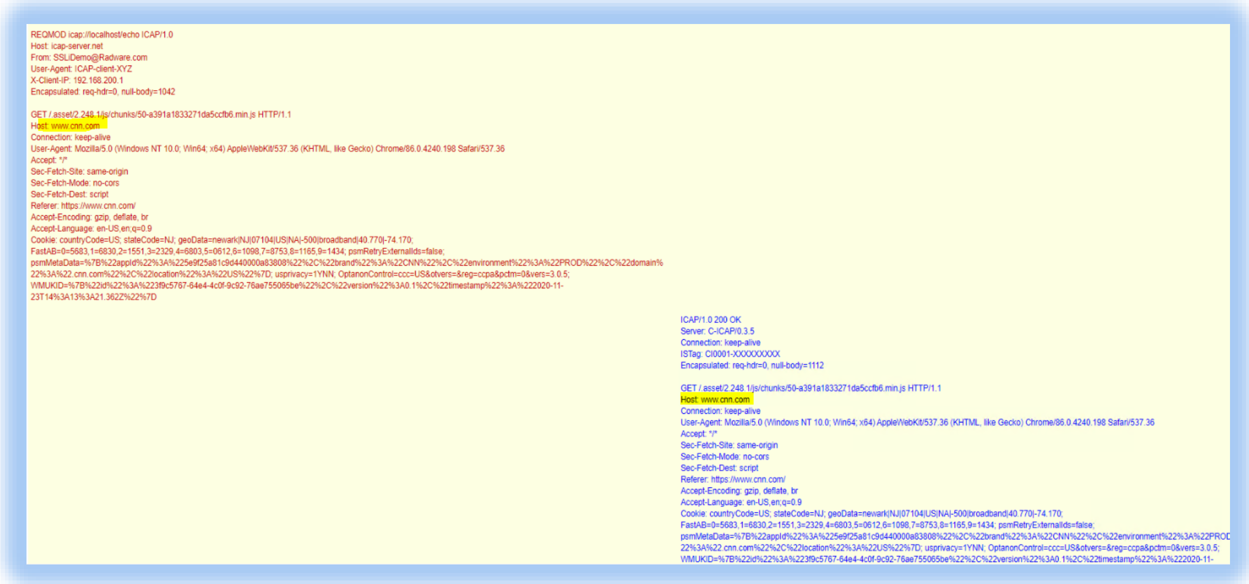


+	tcp	2020/11/23 09:27:08	2020/11/23 09:27:08	192.168.105.2	48837	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:27:03	2020/11/23 09:27:03	192.168.105.2	48836	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:26:58	2020/11/23 09:26:58	192.168.105.2	48835	192.168.105.5	1344	406	7
+	tcp	2020/11/23 09:26:53	2020/11/23 09:26:53	192.168.105.2	48834	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:26:48	2020/11/23 09:26:48	192.168.105.2	48833	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:26:43	2020/11/23 09:26:43	192.168.105.2	48832	192.168.105.5	1344	406	7
+	tcp	2020/11/23 09:26:38	2020/11/23 09:26:38	192.168.105.2	48831	192.168.105.5	1344	406	7
+	tcp	2020/11/23 09:26:33	2020/11/23 09:26:33	192.168.105.2	48830	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:26:28	2020/11/23 09:26:28	192.168.105.2	48829	192.168.105.5	1344	406	7
+	tcp	2020/11/23 09:26:23	2020/11/23 09:26:23	192.168.105.2	48828	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:26:18	2020/11/23 09:26:18	192.168.105.2	48827	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:26:13	2020/11/23 09:26:13	192.168.105.2	48826	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:26:08	2020/11/23 09:26:08	192.168.105.2	48825	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:26:03	2020/11/23 09:26:03	192.168.105.2	48824	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:25:58	2020/11/23 09:25:58	192.168.105.2	48823	192.168.105.5	1344	352	6

6. Scroll down to get ICAP payload:



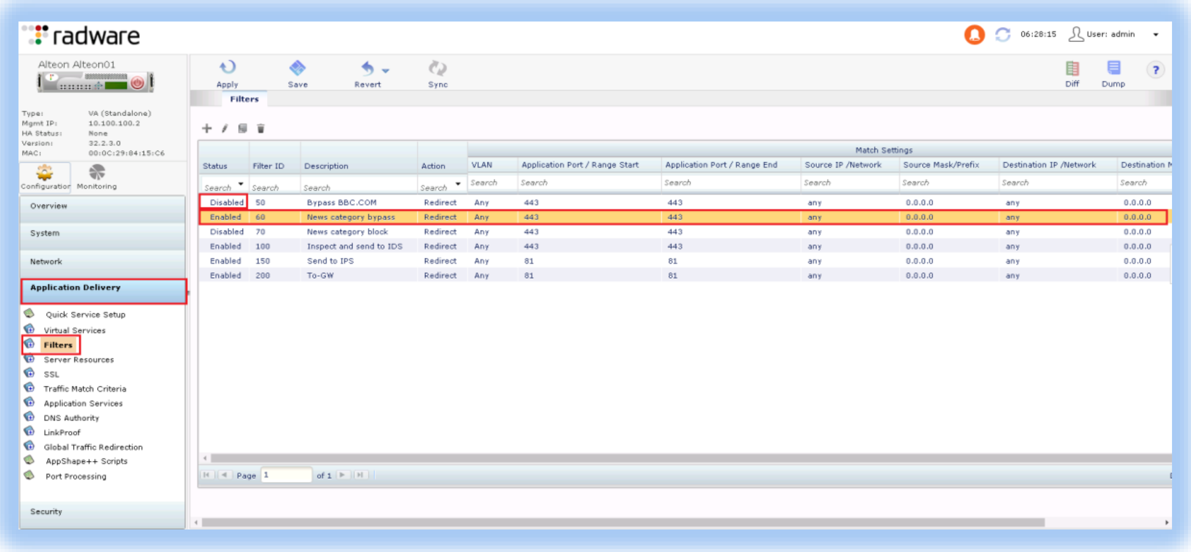
+	tcp	2020/11/22 08:36:44	2020/11/22 08:36:50	192.168.200.1	51460	34.202.178.124	81	Hostname ▾ mms.cnn.com URI ▾ mms.cnn.com/internalheadreq mms.cnn.com/aapJCtJdnQlbiR4JXRueSROJ0xANXBycn4mfSVueHNMQkFHNXBxIUx1cHskdDUjdHV0IyN0I0w1JHQkJHh-fW4jdHV0IyN0I0w1JHQkJHh-fW58dCQkcHZ0bnJ-Jn0ITD81eSdMQT0_PUBAQEQ1cnNyTCh4fXN-KD1uJCFuPXwkdj1ueH0IdCN9cHs9cnNyQDV3I3R1THcUSEkNEJQNEFVNEFVKCgoPXJ9fT1yfnw0QVU1cn59JHR9JWRkWFNMJn1zdHV4fXRzNSU0RFEndCMleHJwezREU0x9dCgk
+	tcp	2020/11/22 08:36:31	2020/11/22 08:41:33	192.168.200.1	51450	96.6.28.230	81	Hostname ▾ dynaimage.cdn.cnn.com URI ▾ dynaimage.cdn.cnn.com/internalheadreq dynaimage.cdn.cnn.com/cnn/animations/w_162/201117182207-desktop-diplomat-saves-drowning-woman.mp4
+	tcp	2020/11/22 08:36:00	2020/11/22 08:37:01	192.168.200.1	51398	151.101.1.67	81	Hostname ▾ www.cnn.com URI ▾ www.cnn.com/internalheadreq
+	tcp	2020/11/22 08:36:00	2020/11/22 08:37:01	192.168.200.1	51399	151.101.1.67	81	Hostname ▾ www.cnn.com URI ▾ www.cnn.com/internalheadreq
+	tcp	2020/11/22 08:36:00	2020/11/22 08:37:01	192.168.200.1	51397	151.101.1.67	81	Hostname ▾ www.cnn.com URI ▾ www.cnn.com/internalheadreq
+	tcp	2020/11/22 08:36:00	2020/11/22 08:37:01	192.168.200.1	51396	151.101.1.67	81	Hostname ▾ www.cnn.com URI ▾ www.cnn.com/internalheadreq
+	tcp	2020/11/22 08:35:14	2020/11/22 08:35:51	192.168.200.1	51321	3.219.249.186	81	Hostname ▾ smetrics.cnn.com URI ▾ smetrics.cnn.com/b/ss/cnn-adbp-domestic/1/JS-2.17.0/s8106477631678?AQB=1&ndh=1&pf=1&t=22%2F10%2F2020%208%3A56%3A55%200%20300&mid=17750144456030505314469241743872552347&aid=2FDD352E05158566-6000060FB2E0B4C6&aamlh=7&ce=UTF-8&ns=cnn&pageName=cnn%3Ao%3A%2F&g=https%3A%2F%2Fwww.cnn.com%2F&c.&cm.&ssf=1&.cm&.c&cc=USD&server=cnn.com&events=event26&aamb=RKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y&l1=16b6&l2=&c8=new%3A1&v8=D%3Dc8&v15=0%3D8438%2C1%3D7241%2C2%3D8671%2C3%3D8733%2C4%3D0599%2C5%3D3556%2C6%3D6959%2C7%3D8701%2C8%3D4612%2C9%3D3739&v22=0&c26=www.cnn.com%2F&v26=D%3DpageName&c28=%3A&v28=D%3Dc28&v29=D%3Dserver&c30=cnn%20domestic&v30=D%3Dc30&c33=adbp%3Anone&v33=D%3Dc33&c35=cnn.prod.46.20201030&v35=D%3Dc35&v36=Nx5zBtvY&c37=desktop&v37=D%3Dc37&c44=section_homepage1&v44=news&c46=16060534044426876294726858&v46=D%3Dc46&c47=5fba3ba000ff2a0a3f86cd0016c86030&v47=D%3Dc47&c48=topics%20available&c51=anonymous&v51=D%3Dc51&c56=landscape&v56=D%3Dc56&c57=no%20mvpd%20set&v57=D%3Dc57&c59=no%20mvpd%20set&v59=D%3Dc59&c64=cnn%20news&v64=D%3Dc64&c74=account%20not%20verified&v74=D%3Dc74&c75=nvs&v75=D%3Dc75&v89=not%20logged%20in&v195=5480007220231978004&v196=2aaaca62-c35f-4cc9-ad6f-869366a509c2&v197=91513f1c-ca74-4984-85a0-c3ad35d61031&s=1920x1080&c=24&j=1.6&v=N&k=Y&bw=1920&bh=937&mcorgid=7FF852E2556756057F000101%40AdobeOrg&AQE=1 smetrics.cnn.com/internalheadreq



```
REQMOD icap://localhost/echo ICAP/1.0
Host: icap-server.net
From: SSLiDemo@Radware.com
User-Agent: ICAP-client-XYZ
X-Client-IP: 192.168.200.1
Encapsulated: req-hdr=0, null-body=1042

GET /.asset/2.248.1/js/chunks/50-a391a1833271da5ccfb6.min.js HTTP/1.1
Host: www.cnn.com
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.198 Safari/537.36
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://www.cnn.com/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: countryCode=US; stateCode=NJ; geoData=newark|NJ|07104|US|NA|-500|broadband|40.770|-74.170;
FastAB=0=5683,1=6830,2=1551,3=2329,4=6803,5=0612,6=1098,7=8753,8=1165,9=1434; psmRetryExternalIds=false;
psmMetaData=%7B%22appId%22%3A%225e9f25a81c9d440000a83808%22%2C%22brand%22%3A%22CNN%22%2C%22environment%22%3A%22PROD%22%2C%22domain%
22%3A%22.cnn.com%22%2C%22location%22%3A%22US%22%7D; usprivacy=1YNN; OptanonControl=ccc=US&otvers=&reg=ccpa&pctm=0&vers=3.0.5;
WMUKID=%7B%22id%22%3A%223f9c5767-64e4-4c0f-9c92-76ae755065be%22%2C%22version%22%3A0.1%2C%22timestamp%22%3A%222020-11-
23T14%3A13%3A21.362Z%22%7D
```

```
ICAP/1.0 200 OK
Server: C-ICAP/0.3.5
Connection: keep-alive
ISTag: CI0001-XXXXXXXXX
Encapsulated: req-hdr=0, null-body=1112

GET /.asset/2.248.1/js/chunks/50-a391a1833271da5ccfb6.min.js HTTP/1.1
Host: www.cnn.com
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.198 Safari/537.36
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://www.cnn.com/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: countryCode=US; stateCode=NJ; geoData=newark|NJ|07104|US|NA|-500|broadband|40.770|-74.170;
FastAB=0=5683,1=6830,2=1551,3=2329,4=6803,5=0612,6=1098,7=8753,8=1165,9=1434; psmRetryExternalIds=false;
psmMetaData=%7B%22appId%22%3A%225e9f25a81c9d440000a83808%22%2C%22brand%22%3A%22CNN%22%2C%22environment%22%3A%22PROD
22%3A%22.cnn.com%22%2C%22location%22%3A%22US%22%7D; usprivacy=1YNN; OptanonControl=ccc=US&otvers=&reg=ccpa&pctm=0&vers=3.0.5;
WMUKID=%7B%22id%22%3A%223f9c5767-64e4-4c0f-9c92-76ae755065be%22%2C%22version%22%3A0.1%2C%22timestamp%22%3A%222020-11-
```

7. Enable **bypass** filter for **NEWS category**:
   - Login to the Alteon
   - Navigate to **Application Delivery → Filters**
   - Disable filter **50**
   - Enable filter **60**



Alteon Alteon01

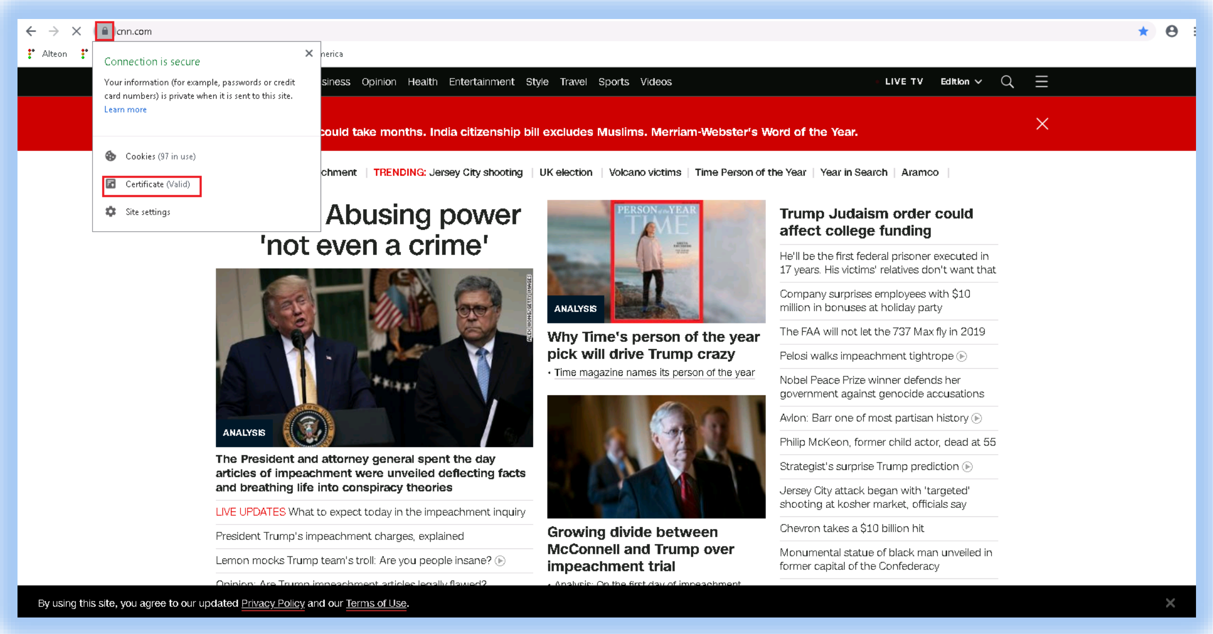
Type:	VA (Standalone)
Mgmt IP:	10.100.100.2
HA Status:	None
Version:	32.2.3.0
MAC:	00:0C:29:84:15:C6

				Match Settings						
Status	Filter ID	Description	Action	VLAN	Application Port / Range Start	Application Port / Range End	Source IP /Network	Source Mask/Prefix	Destination IP /Network	Destination M
Disabled	50	Bypass BBC.COM	Redirect	Any	443	443	any	0.0.0.0	any	0.0.0.0
Enabled	60	News category bypass	Redirect	Any	443	443	any	0.0.0.0	any	0.0.0.0
Disabled	70	News category block	Redirect	Any	443	443	any	0.0.0.0	any	0.0.0.0
Enabled	100	Inspect and send to IDS	Redirect	Any	443	443	any	0.0.0.0	any	0.0.0.0
Enabled	150	Send to IPS	Redirect	Any	81	81	any	0.0.0.0	any	0.0.0.0
Enabled	200	To-GW	Redirect	Any	81	81	any	0.0.0.0	any	0.0.0.0

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided "as is". Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness or performance

8. Click on **CNN** bookmark again then click on the **Lock Button** and then **Certificate** to verify the certificate issuer:



Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

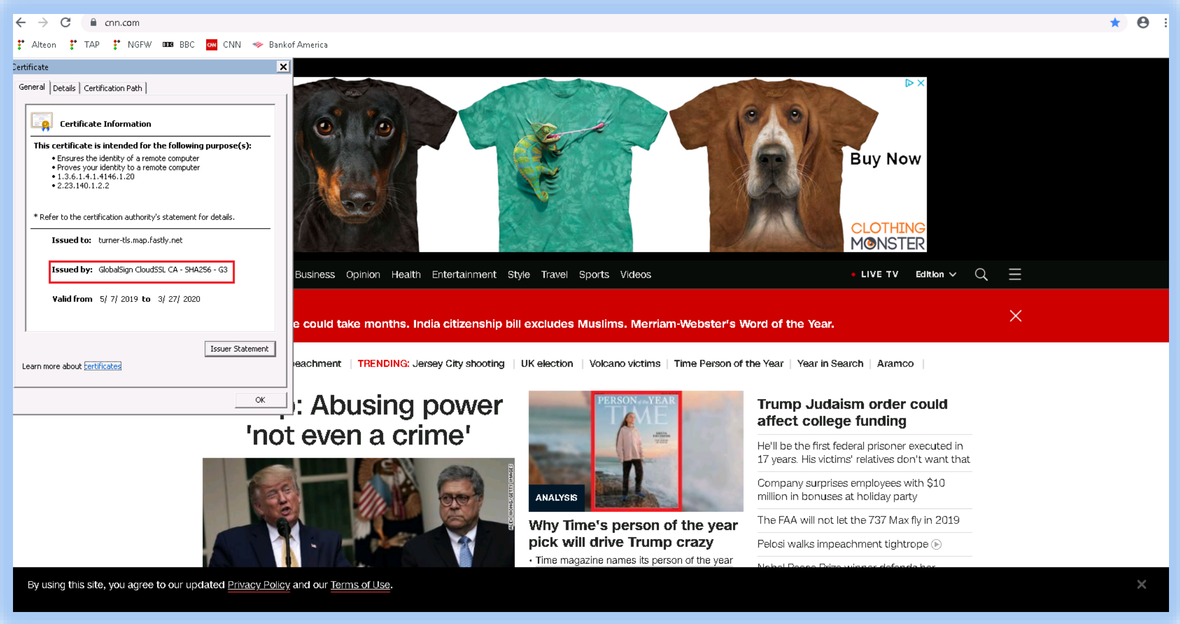
Cookies (97 in use)

Certificate (Valid)

Site settings

cnn.com
Alteon
Business Opinion Health Entertainment Style Travel Sports Videos
LIVE TV Edition
could take months. India citizenship bill excludes Muslims. Merriam-Webster's Word of the Year.
TRENDING: Jersey City shooting | UK election | Volcano victims | Time Person of the Year | Year in Search | Aramco
Abusing power 'not even a crime'
ANALYSIS
The President and attorney general spent the day articles of impeachment were unveiled deflecting facts and breathing life into conspiracy theories
LIVE UPDATES What to expect today in the impeachment inquiry
President Trump's impeachment charges, explained
Lemon mocks Trump team's troll: Are you people insane?
Why Time's person of the year pick will drive Trump crazy
Time magazine names its person of the year
Growing divide between McConnell and Trump over impeachment trial
Trump Judaism order could affect college funding
He'll be the first federal prisoner executed in 17 years. His victims' relatives don't want that
Company surprises employees with $10 million in bonuses at holiday party
The FAA will not let the 737 Max fly in 2019
Pelosi walks impeachment tightrope
Nobel Peace Prize winner defends her government against genocide accusations
Avlon: Barr one of most partisan history
Philip McKeon, former child actor, dead at 55
Strategist's surprise Trump prediction
Jersey City attack began with 'targeted' shooting at kosher market, officials say
Chevron takes a $10 billion hit
Monumental statue of black man unveiled in former capital of the Confederacy
By using this site, you agree to our updated Privacy Policy and our Terms of Use.

9. We can see that the **certificate wasn't issued by Alteon** which means the **request was served directly from the web server**, effectively **bypassing the SSL inspection**:



Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- 1.3.6.1.4.1.4146.1.20
- 2.23.140.1.2.2

* Refer to the certification authority's statement for details.

Issued to: turner-tls.map.fastly.net

Issued by: GlobalSign CloudSSL CA - SHA256 - G3

Valid from 5/ 7/ 2019 **to** 3/ 27/ 2020

Issuer Statement

Learn more about certificates

OK

e could take months. India citizenship bill excludes Muslims. Merriam-Webster's Word of the Year.

eachment | TRENDING: Jersey City shooting | UK election | Volcano victims | Time Person of the Year | Year in Search | Aramco

: Abusing power 'not even a crime'

Why Time's person of the year pick will drive Trump crazy

• Time magazine names its person of the year

Trump Judaism order could affect college funding

He'll be the first federal prisoner executed in 17 years. His victims' relatives don't want that

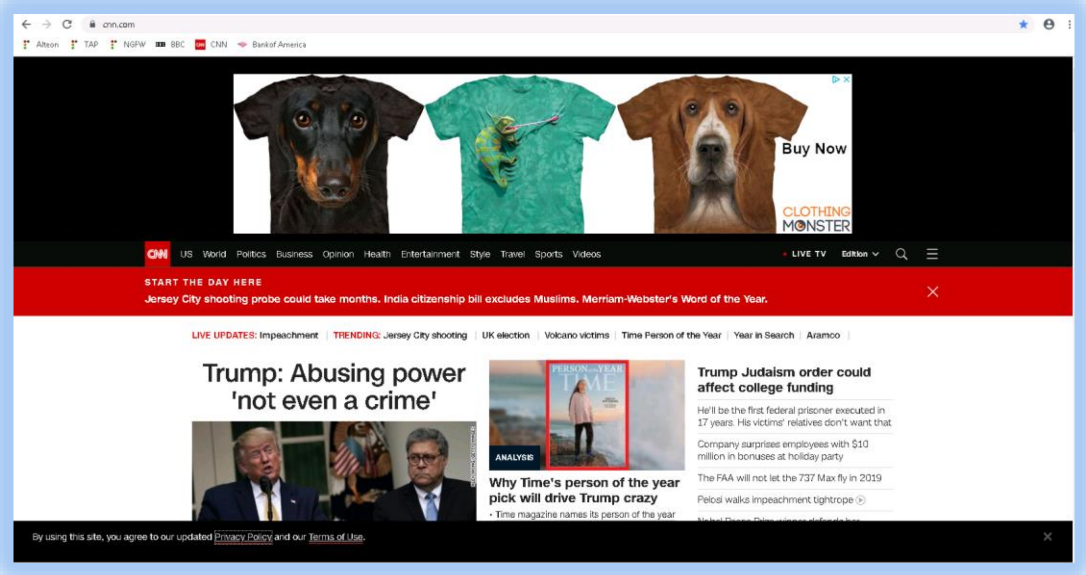
Company surprises employees with $10 million in bonuses at holiday party

The FAA will not let the 737 Max fly in 2019

Pelosi walks impeachment tightrope

By using this site, you agree to our updated Privacy Policy and our Terms of Use.

10. Click on **Bank of America** bookmark:



START THE DAY HERE

Jersey City shooting probe could take months. India citizenship bill excludes Muslims. Merriam-Webster's Word of the Year.

LIVE UPDATES: Impeachment | TRENDING: Jersey City shooting | UK election | Volcano victims | Time Person of the Year | Year in Search | Aramco

Trump: Abusing power 'not even a crime'

Why Time's person of the year pick will drive Trump crazy

• Time magazine names its person of the year

Trump Judaism order could affect college funding

He'll be the first federal prisoner executed in 17 years. His victims' relatives don't want that

Company surprises employees with $10 million in bonuses at holiday party

The FAA will not let the 737 Max fly in 2019

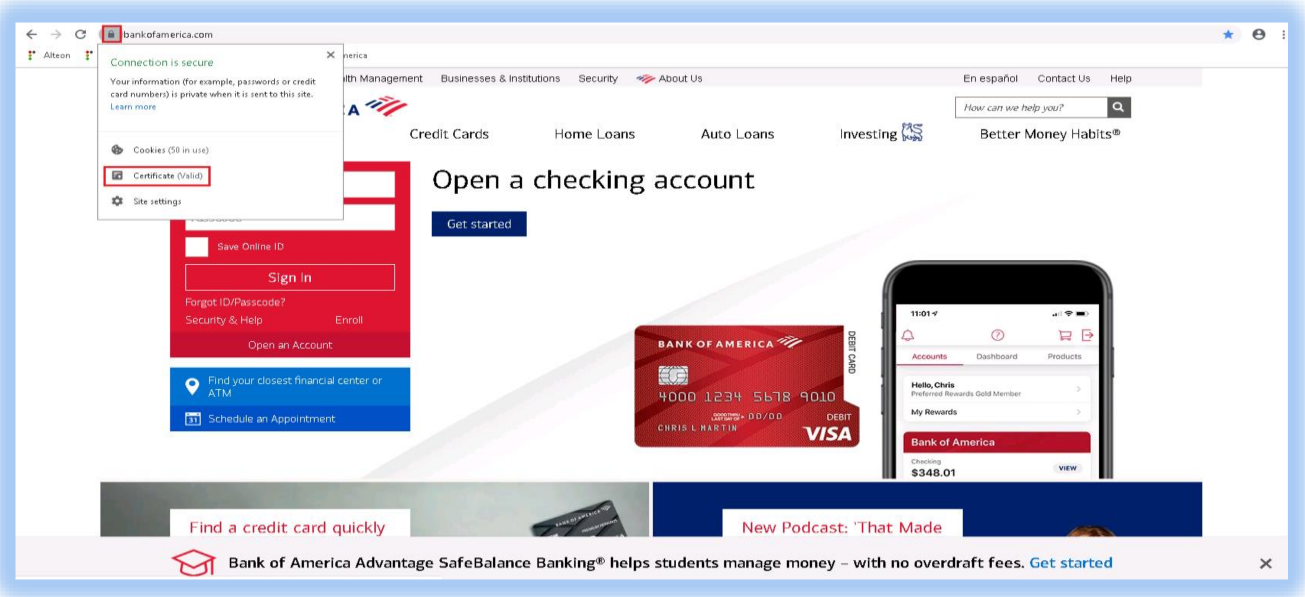
Pelosi walks impeachment tightrope

By using this site, you agree to our updated Privacy Policy and our Terms of Use.

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided "as is". Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness or performance

11. Click on the **Lock Button** and then **Certificate** button to verify the certificate issuer:



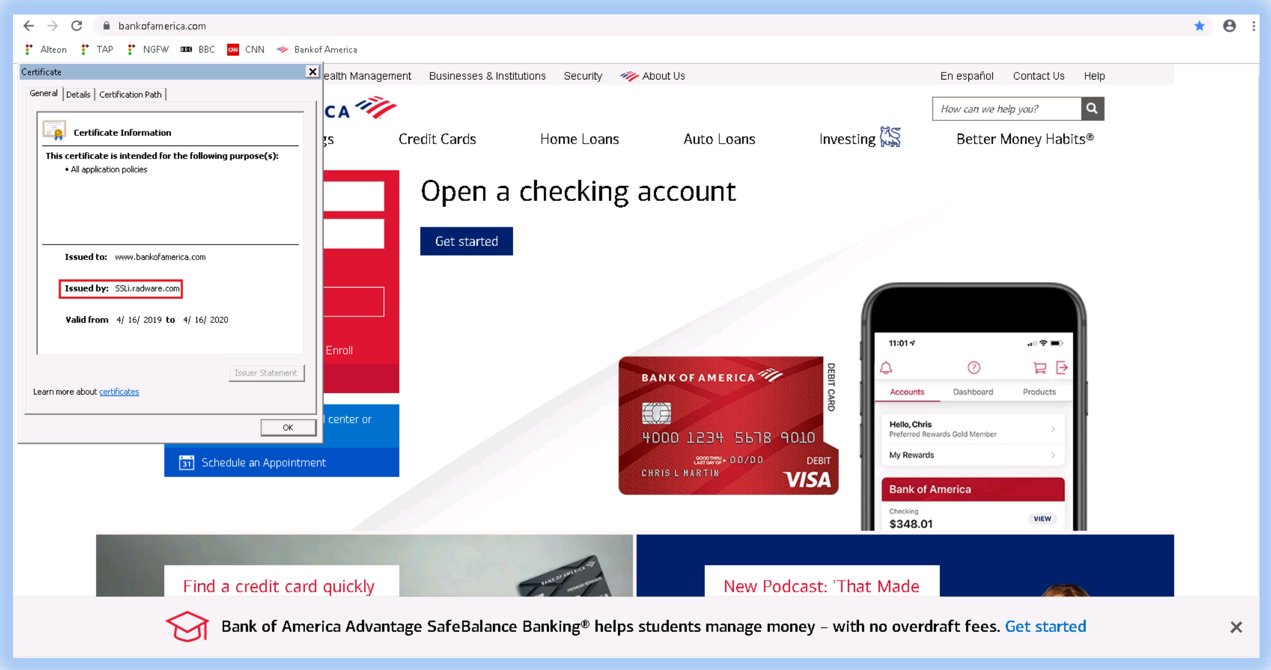
bankofamerica.com

Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

Bank of America Advantage SafeBalance Banking® helps students manage money – with no overdraft fees. Get started

12. We can see that the **certificate was issued by the Alteon**, meaning the **traffic was forwarded to security devices for inspection** and re-encrypted successfully.



Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):
- All application policies

Issued to: www.bankofamerica.com

Issued by: SSLi.radware.com

Valid from 4/ 16/ 2019 to 4/ 16/ 2020

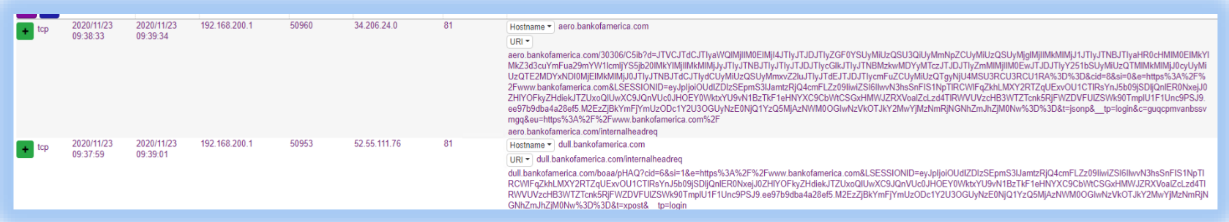
Issuer Statement

Learn more about certificates

OK

Bank of America Advantage SafeBalance Banking® helps students manage money – with no overdraft fees. Get started

13. Browse to "TAP" bookmark in order to watch traffic reaching the "TAP" device:

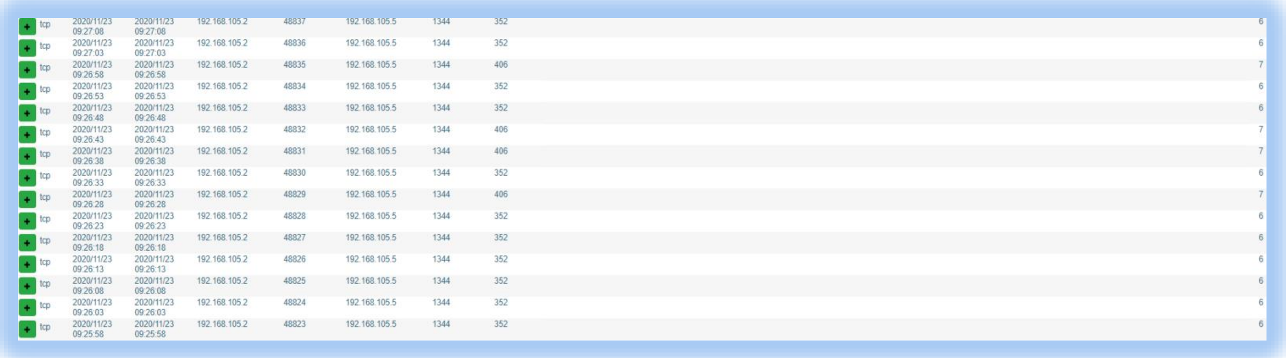


+	tcp	2020/11/23 09:38:33	2020/11/23 09:39:34	192.168.200.1	50960	34.206.24.0	81	Hostname ▾ aero.bankofamerica.com URI ▾ aero.bankofamerica.com/30306/C5ib?d=JTVCJTdCJTIyaWQlMjIlM0ElMjI4JTIyJTJDJTIyZGF0YSUyMiUzQSU3QiUyMmNpZCUyMiUzQSUyMjglMjIlMkMlMjJ1JTIyJTNBJTIyaHR0cHMlM0ElMkYlMkZ3d3cuYmFua29mYW1lcmljYS5jb20lMkYlMjIlMkMlMjJyJTIyJTNBJTIyJTIyJTJDJTIycGlkJTIyJTNBMzkwMDYyMTczJTJDJTIyZmMlMjIlM0EwJTJDJTIyY251bSUyMiUzQTMlMkMlMjJ0cyUyMiUzQTE2MDYxNDI0MjElMkMlMjJ0JTIyJTNBJTdCJTIydCUyMiUzQSUyMmxvZ2luJTIyJTdEJTJDJTIycmFuZCUyMiUzQTgyNjU4MSU3RCU3RCU1RA%3D%3D&cid=8&si=0&e=https%3A%2F%2Fwww.bankofamerica.com&LSESSIONID=eyJpljoiOUdIZDIzSEpmS3IJamtzRjQ4cmFLZz09IiwiZSI6IlwvN3hsSnFIS1NpTIRCWlFqZkhLMXY2RTZqUExvOU1CTIRsYnJ5b09jSDljQnlER0NxejJ0ZHlYOFkyZHdiekJTZUxoQlUwXC9JQnVUc0JHOEY0WktxYU9vN1BzTkF1eHNYXC9CbWtCSGxHMWJZRXVoalZcLzd4TlRWVUVzcHB3WTZTcnk5RjFWZDVFUlZSWk90TmplU1F1Unc9PSJ9.ee97b9dba4a28ef5.M2EzZjBkYmFjYmUzODc1Y2U3OGUyNzE0NjQ1YzQ5MjAzNWM0OGIwNzVkOTJkY2MwYjMzNmRjNGNhZmJhZjM0Nw%3D%3D&t=jsonp&__tp=login&c=guqcpmvanbssvmgq&eu=https%3A%2F%2Fwww.bankofamerica.com%2F aero.bankofamerica.com/internalheadreq
+	tcp	2020/11/23 09:37:59	2020/11/23 09:39:01	192.168.200.1	50953	52.55.111.76	81	Hostname ▾ dull.bankofamerica.com URI ▾ dull.bankofamerica.com/internalheadreq dull.bankofamerica.com/boaa/pHAQ?cid=6&si=1&e=https%3A%2F%2Fwww.bankofamerica.com&LSESSIONID=eyJpljoiOUdIZDIzSEpmS3IJamtzRjQ4cmFLZz09IiwiZSI6IlwvN3hsSnFIS1NpTIRCWlFqZkhLMXY2RTZqUExvOU1CTIRsYnJ5b09jSDljQnlER0NxejJ0ZHlYOFkyZHdiekJTZUxoQlUwXC9JQnVUc0JHOEY0WktxYU9vN1BzTkF1eHNYXC9CbWtCSGxHMWJZRXVoalZcLzd4TlRWVUVzcHB3WTZTcnk5RjFWZDVFUlZSWk90TmplU1F1Unc9PSJ9.ee97b9dba4a28ef5.M2EzZjBkYmFjYmUzODc1Y2U3OGUyNzE0NjQ1YzQ5MjAzNWM0OGIwNzVkOTJkY2MwYjMzNmRjNGNhZmJhZjM0Nw%3D%3D&t=xpost&__tp=login

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

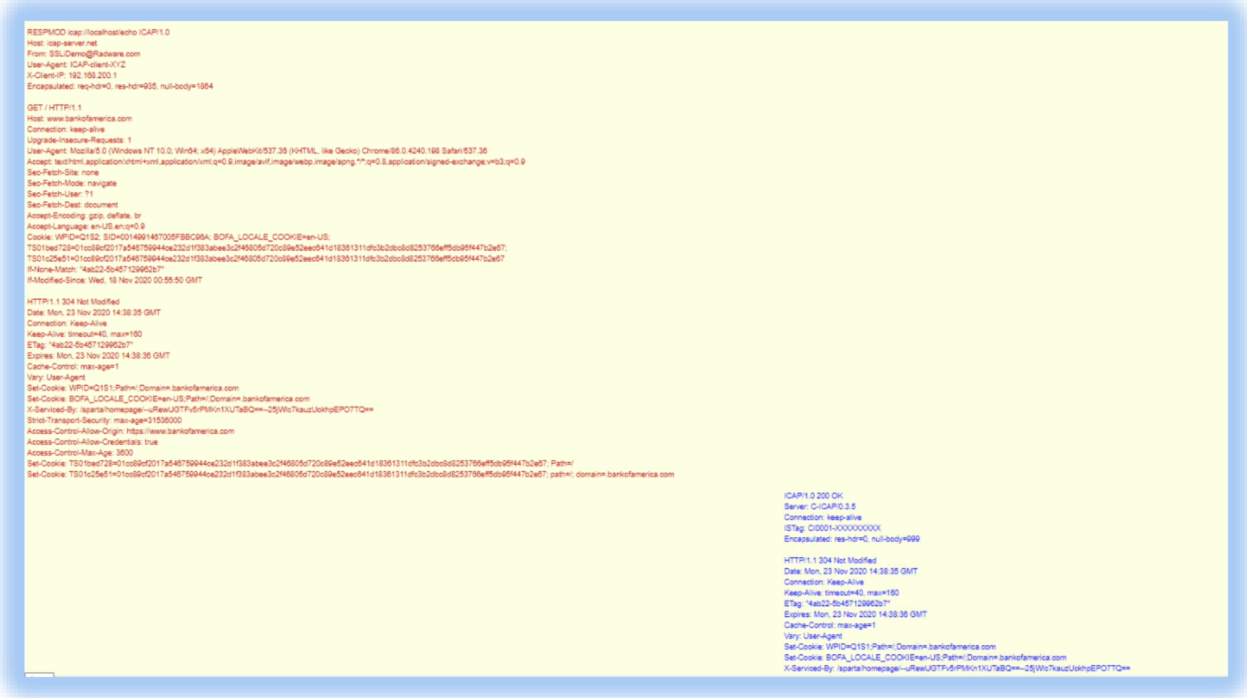
All information provided in the Demo lab and documentation is provided "as is". Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness or performance

14. Browse to "ICAP" bookmark in order to watch traffic reaching the ICAP device and click the "+" button:



+	tcp	2020/11/23 09:27:08	2020/11/23 09:27:08	192.168.105.2	48837	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:27:03	2020/11/23 09:27:03	192.168.105.2	48836	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:26:58	2020/11/23 09:26:58	192.168.105.2	48835	192.168.105.5	1344	406	7
+	tcp	2020/11/23 09:26:53	2020/11/23 09:26:53	192.168.105.2	48834	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:26:48	2020/11/23 09:26:48	192.168.105.2	48833	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:26:43	2020/11/23 09:26:43	192.168.105.2	48832	192.168.105.5	1344	406	7
+	tcp	2020/11/23 09:26:38	2020/11/23 09:26:38	192.168.105.2	48831	192.168.105.5	1344	406	7
+	tcp	2020/11/23 09:26:33	2020/11/23 09:26:33	192.168.105.2	48830	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:26:28	2020/11/23 09:26:28	192.168.105.2	48829	192.168.105.5	1344	406	7
+	tcp	2020/11/23 09:26:23	2020/11/23 09:26:23	192.168.105.2	48828	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:26:18	2020/11/23 09:26:18	192.168.105.2	48827	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:26:13	2020/11/23 09:26:13	192.168.105.2	48826	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:26:08	2020/11/23 09:26:08	192.168.105.2	48825	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:26:03	2020/11/23 09:26:03	192.168.105.2	48824	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:25:58	2020/11/23 09:25:58	192.168.105.2	48823	192.168.105.5	1344	352	6

15. Scroll down to get ICAP payload:



```
RESPMOD icap://localhost/echo ICAP/1.0
Host: icap-server.net
From: SSLiDemo@Radware.com
User-Agent: ICAP-client-XYZ
X-Client-IP: 192.168.200.1
Encapsulated: req-hdr=0, res-hdr=935, null-body=1864

GET / HTTP/1.1
Host: www.bankofamerica.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.198 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: WPID=Q1S2; SID=0014991467005FBBC96A; BOFA_LOCALE_COOKIE=en-US;
TS01bed728=01cc89cf2017a546759944ce232d1f383abee3c2f46805d720c89e52eec641d18361311dfc3b2dbc8d8253766eff5db95f447b2e67;
TS01c25e51=01cc89cf2017a546759944ce232d1f383abee3c2f46805d720c89e52eec641d18361311dfc3b2dbc8d8253766eff5db95f447b2e67
If-None-Match: "4ab22-5b457129962b7"
If-Modified-Since: Wed, 18 Nov 2020 00:55:50 GMT

HTTP/1.1 304 Not Modified
Date: Mon, 23 Nov 2020 14:38:35 GMT
Connection: Keep-Alive
Keep-Alive: timeout=40, max=160
ETag: "4ab22-5b457129962b7"
Expires: Mon, 23 Nov 2020 14:38:36 GMT
Cache-Control: max-age=1
Vary: User-Agent
Set-Cookie: WPID=Q1S1;Path=/;Domain=.bankofamerica.com
Set-Cookie: BOFA_LOCALE_COOKIE=en-US;Path=/;Domain=.bankofamerica.com
X-Serviced-By: /sparta/homepage/--uRewUGTFv5rPMKn1XUTaBQ==--25jWlc7kauzUokhpEPO7TQ==
Strict-Transport-Security: max-age=31536000
Access-Control-Allow-Origin: https://www.bankofamerica.com
Access-Control-Allow-Credentials: true
Access-Control-Max-Age: 3600
Set-Cookie: TS01bed728=01cc89cf2017a546759944ce232d1f383abee3c2f46805d720c89e52eec641d18361311dfc3b2dbc8d8253766eff5db95f447b2e67; Path=/
Set-Cookie: TS01c25e51=01cc89cf2017a546759944ce232d1f383abee3c2f46805d720c89e52eec641d18361311dfc3b2dbc8d8253766eff5db95f447b2e67; path=/; domain=.bankofamerica.com

ICAP/1.0 200 OK
Server: C-ICAP/0.3.5
Connection: keep-alive
ISTag: CI0001-XXXXXXXXX
Encapsulated: res-hdr=0, null-body=999

HTTP/1.1 304 Not Modified
Date: Mon, 23 Nov 2020 14:38:35 GMT
Connection: Keep-Alive
Keep-Alive: timeout=40, max=160
ETag: "4ab22-5b457129962b7"
Expires: Mon, 23 Nov 2020 14:38:36 GMT
Cache-Control: max-age=1
Vary: User-Agent
Set-Cookie: WPID=Q1S1;Path=/;Domain=.bankofamerica.com
Set-Cookie: BOFA_LOCALE_COOKIE=en-US;Path=/;Domain=.bankofamerica.com
X-Serviced-By: /sparta/homepage/--uRewUGTFv5rPMKn1XUTaBQ==--25jWlc7kauzUokhpEPO7TQ==
```

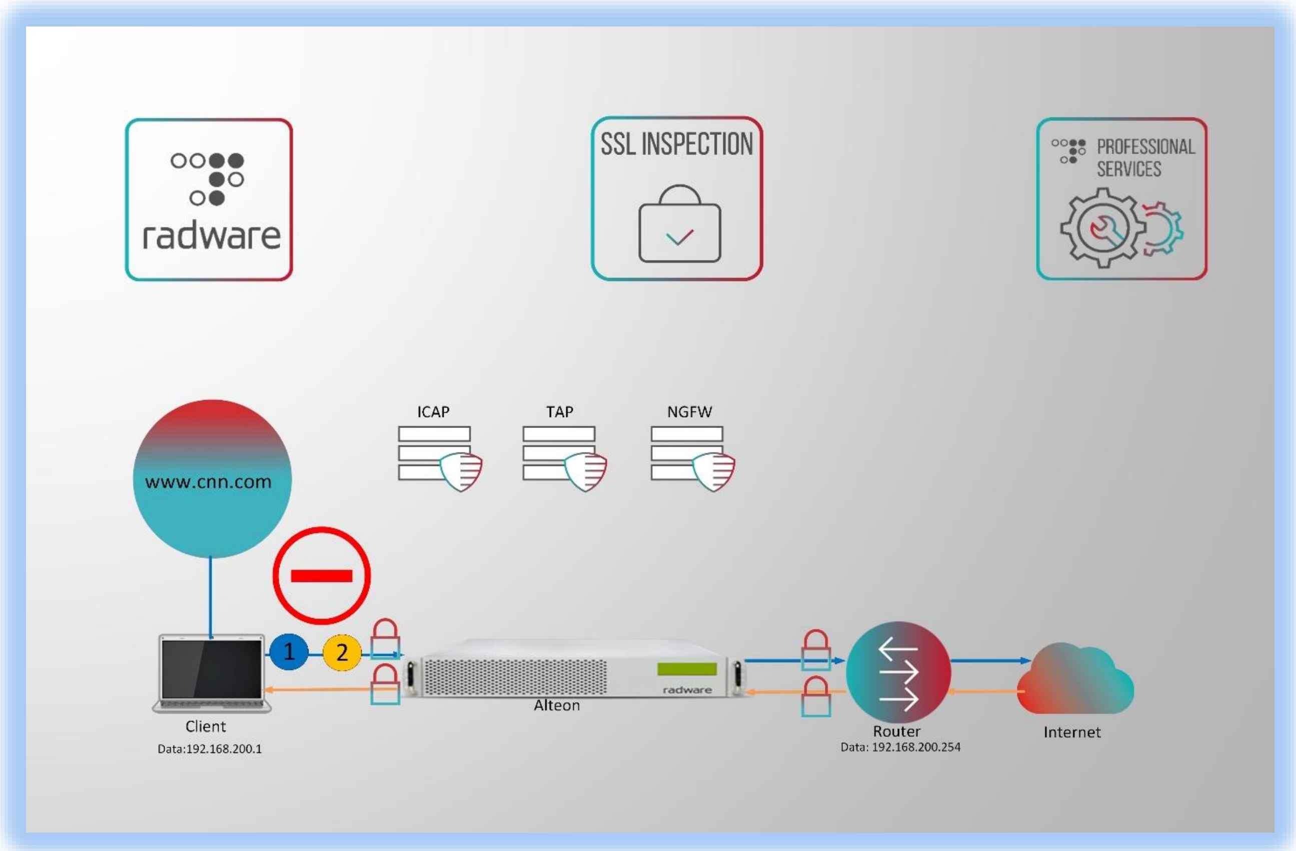
4. Scenario 4 – Category Based Block

In this scenario we will demonstrate blocking specific category of web sites

Note:

In order to view the Alteon configuration refer to Appendix H: Scenario 4 Configuration
Please Open SSL Inspection analytics using Appendix I: Vision SSL Inspection Analytics

Diagram and Traffic Flow



The diagram below details the entire flow of the traffic:

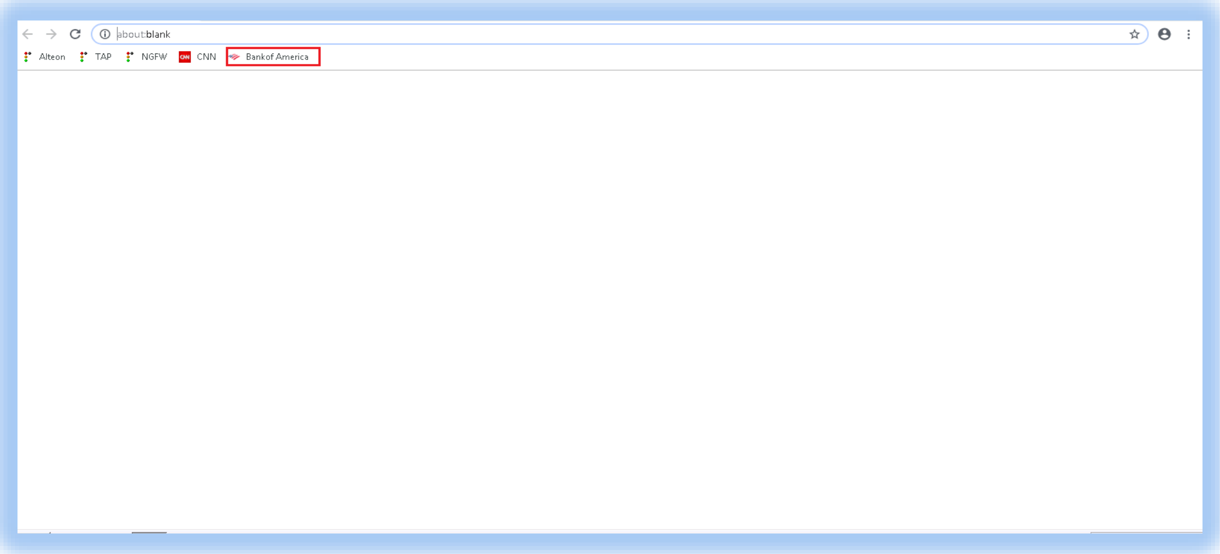
1. The client browses to www.cnn.com.
2. Based on web category filter the Alteon blocks the traffic and responds with a sorry page.

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

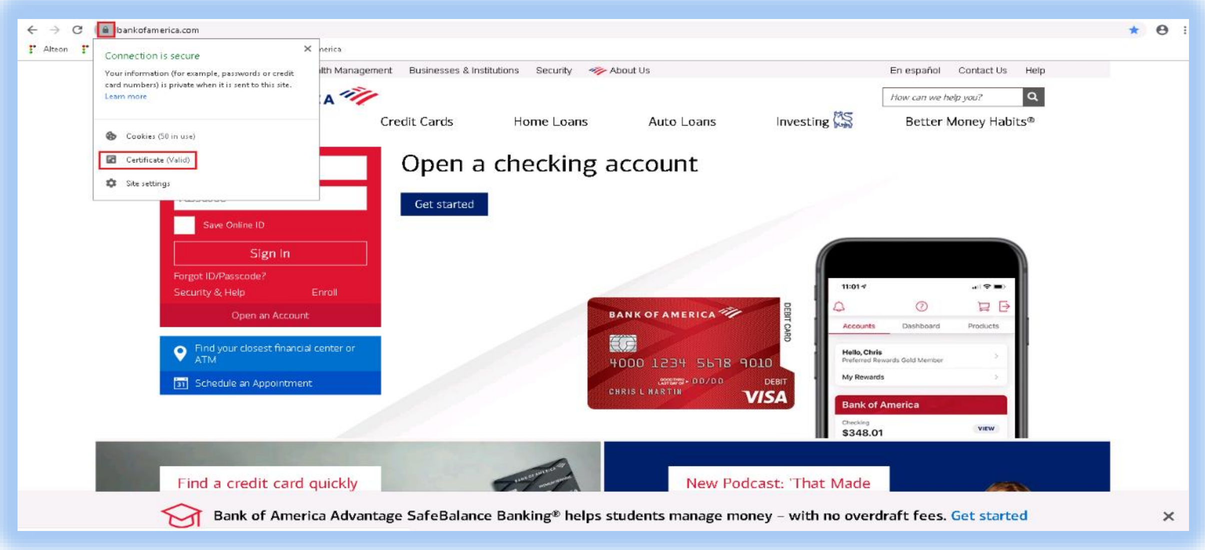
All information provided in the Demo lab and documentation is provided “as is”. Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness or performance

Running the Demo Scenario

1. Open Chrome browser and Click on **Bank of America** bookmark:



2. Click on the **Lock Button** and then **Certificate** to verify the certificate issuer:



Connection is secure

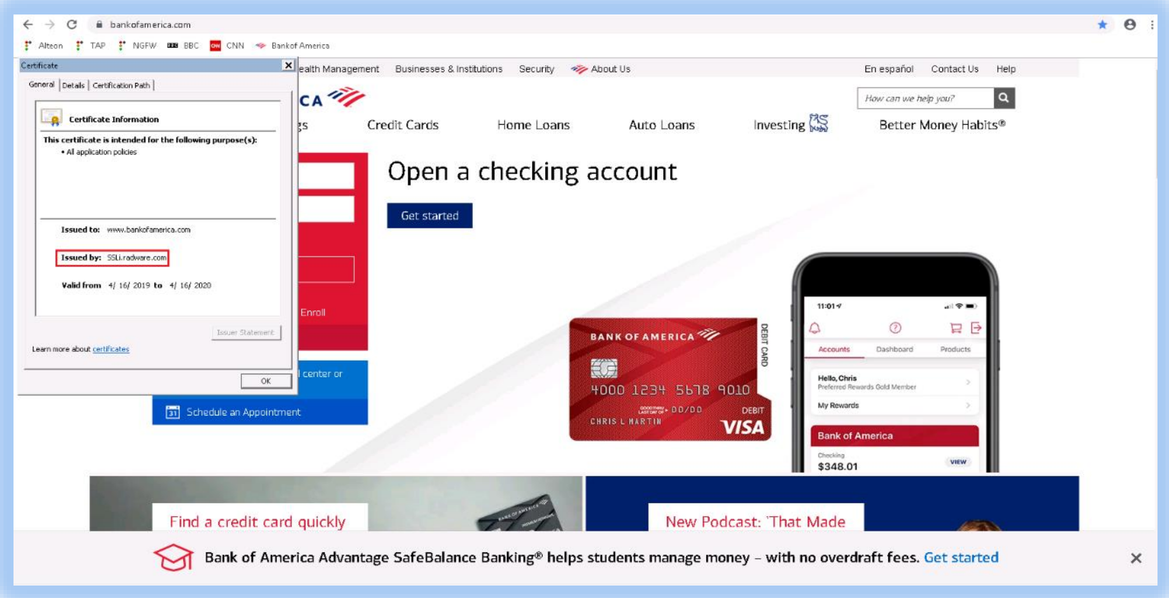
Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

Bank of America Advantage SafeBalance Banking® helps students manage money – with no overdraft fees. Get started

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided "as is". Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness or performance

3. We can see that the certificate was **issued by the Alteon**, meaning the traffic was **forwarded to security devices for inspection** and re-encrypted successfully:



Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):
- All application policies

Issued to: www.bankofamerica.com

Issued by: SSLi.radware.com

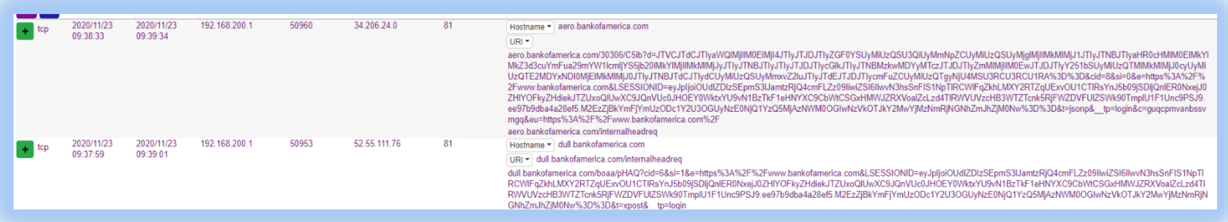
Valid from 4/ 16/ 2019 to 4/ 16/ 2020

Issuer Statement

Learn more about certificates

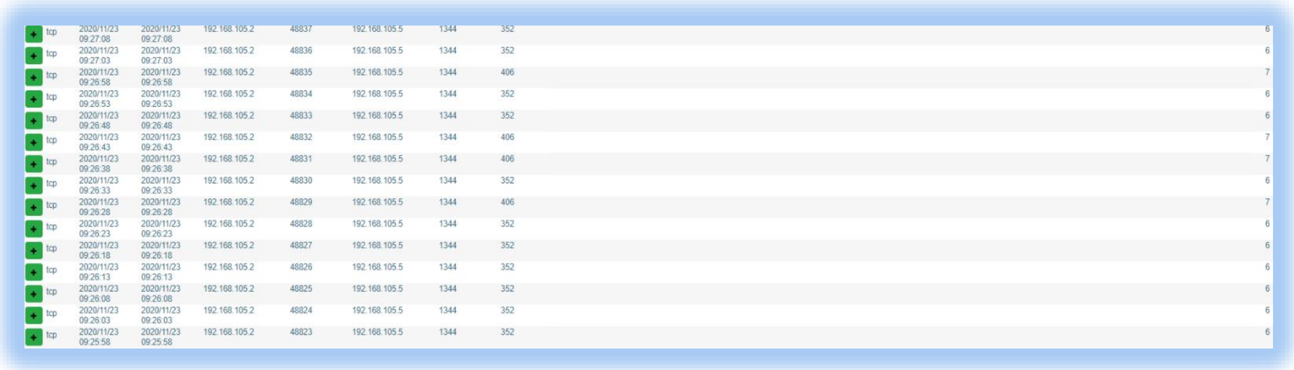
OK

4. Browse to "TAP" bookmark in order to watch traffic reaching the "TAP" device:



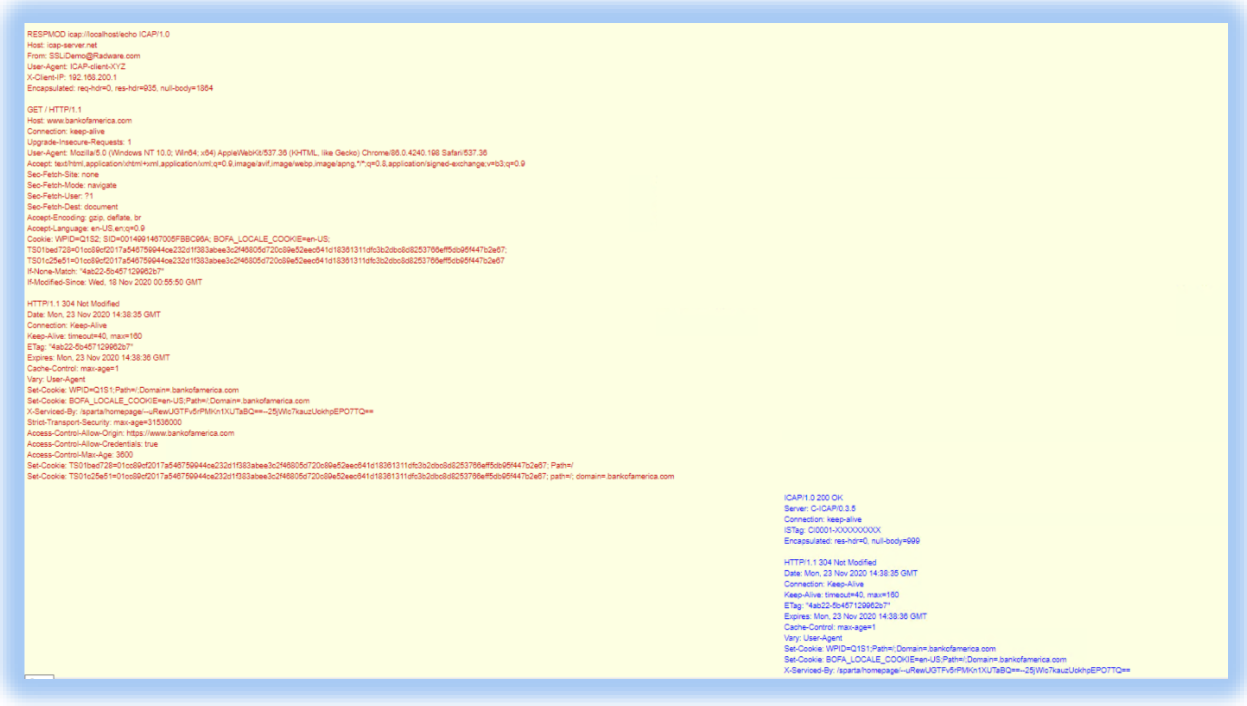
+	tcp	2020/11/23 09:38:33	2020/11/23 09:39:34	192.168.200.1	50960	34.206.24.0	81	Hostname ▾ aero.bankofamerica.com URI ▾ aero.bankofamerica.com/30306/C5ib?d=JTVCJTdCJTIyaWQlMjIlM0ElMjI4JTIyJTJDJTIyZGF0YSUyMiUzQSU3QiUyMmNpZCUyMiUzQSUyMjglMjIlMkMlMjJ1JTIyJTNBJTIyaHR0cHMlM0ElMkYlMkZ3d3cuYmFua29mYW1lcmljYS5jb20lMkYlMjIlMkMlMjJyJTIyJTNBJTIyJTIyJTJDJTIycGlkJTIyJTNBMzkwMDYyMTczJTJDJTIyZmMlMjIlM0EwJTJDJTIyY251bSUyMiUzQTMlMkMlMjJ0cyUyMiUzQTE2MDYxNDI0MjElMkMlMjJ0JTIyJTNBJTdCJTIydCUyMiUzQSUyMmxvZ2luJTIyJTdEJTJDJTIycmFuZCUyMiUzQTgyNjU4MSU3RCU3RCU1RA%3D%3D&cid=8&si=0&e=https%3A%2F%2Fwww.bankofamerica.com&LSESSIONID=eyJpljoiOUdIZDIzSEpmS3lJamtzRjQ4cmFLZz09liwiZSI6IlwvN3hsSnFIS1NpTlRCWlFqZkhLMXY2RTZqUExvOU1CTlRsYnJ5b09jSDljQnlER0NxejJ0ZHlYOFkyZHdiekJTZUxoQlUwXC9JQnVUc0JHOEY0WktxYU9vN1BzTkF1eHNYXC9CbWtCSGxHMWJZRXVoalZcLzd4TlRWVUVzcHB3WTZTcnk5RjFWZDVFUlZSWk90TmplU1F1Unc9PSJ9.ee97b9dba4a28ef5.M2EzZjBkYmFjYmUzODc1Y2U3OGUyNzE0NjQ1YzQ5MjAzNWM0OGIwNzVkOTJkY2MwYjMzNmRjNGNhZmJhZjM0Nw%3D%3D&t=jsonp&__tp=login&c=guqcpmvanbssvmgq&eu=https%3A%2F%2Fwww.bankofamerica.com%2F aero.bankofamerica.com/internalheadreq
+	tcp	2020/11/23 09:37:59	2020/11/23 09:39:01	192.168.200.1	50953	52.55.111.76	81	Hostname ▾ dull.bankofamerica.com URI ▾ dull.bankofamerica.com/internalheadreq dull.bankofamerica.com/boaa/pHAQ?cid=6&si=1&e=https%3A%2F%2Fwww.bankofamerica.com&LSESSIONID=eyJpljoiOUdIZDIzSEpmS3lJamtzRjQ4cmFLZz09liwiZSI6IlwvN3hsSnFIS1NpTlRCWlFqZkhLMXY2RTZqUExvOU1CTlRsYnJ5b09jSDljQnlER0NxejJ0ZHlYOFkyZHdiekJTZUxoQlUwXC9JQnVUc0JHOEY0WktxYU9vN1BzTkF1eHNYXC9CbWtCSGxHMWJZRXVoalZcLzd4TlRWVUVzcHB3WTZTcnk5RjFWZDVFUlZSWk90TmplU1F1Unc9PSJ9.ee97b9dba4a28ef5.M2EzZjBkYmFjYmUzODc1Y2U3OGUyNzE0NjQ1YzQ5MjAzNWM0OGIwNzVkOTJkY2MwYjMzNmRjNGNhZmJhZjM0Nw%3D%3D&t=xpost&__tp=login

5. Browse to "ICAP" bookmark in order to watch traffic reaching the ICAP device and click the "+" button:



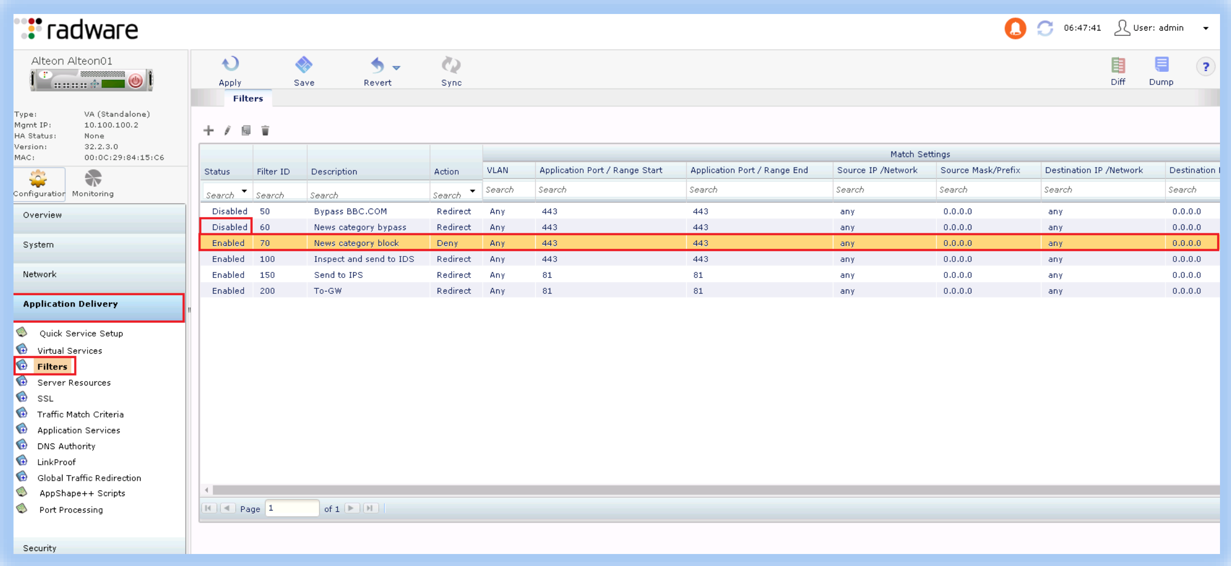
+	tcp	2020/11/23 09:27:08	2020/11/23 09:27:08	192.168.105.2	48837	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:27:03	2020/11/23 09:27:03	192.168.105.2	48836	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:26:58	2020/11/23 09:26:58	192.168.105.2	48835	192.168.105.5	1344	406	7
+	tcp	2020/11/23 09:26:53	2020/11/23 09:26:53	192.168.105.2	48834	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:26:48	2020/11/23 09:26:48	192.168.105.2	48833	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:26:43	2020/11/23 09:26:43	192.168.105.2	48832	192.168.105.5	1344	406	7
+	tcp	2020/11/23 09:26:38	2020/11/23 09:26:38	192.168.105.2	48831	192.168.105.5	1344	406	7
+	tcp	2020/11/23 09:26:33	2020/11/23 09:26:33	192.168.105.2	48830	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:26:28	2020/11/23 09:26:28	192.168.105.2	48829	192.168.105.5	1344	406	7
+	tcp	2020/11/23 09:26:23	2020/11/23 09:26:23	192.168.105.2	48828	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:26:18	2020/11/23 09:26:18	192.168.105.2	48827	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:26:13	2020/11/23 09:26:13	192.168.105.2	48826	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:26:08	2020/11/23 09:26:08	192.168.105.2	48825	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:26:03	2020/11/23 09:26:03	192.168.105.2	48824	192.168.105.5	1344	352	6
+	tcp	2020/11/23 09:25:58	2020/11/23 09:25:58	192.168.105.2	48823	192.168.105.5	1344	352	6

6. Scroll down to get ICAP payload:



```
RESPMOD icap://localhost/echo ICAP/1.0
Host: icap-server.net
From: SSLiDemo@Radware.com
User-Agent: ICAP-client-XYZ
X-Client-IP: 192.168.200.1
Encapsulated: req-hdr=0, res-hdr=935, null-body=1864

GET / HTTP/1.1
Host: www.bankofamerica.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.198 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: WPID=Q1S2; SID=0014991467005FBBC96A; BOFA_LOCALE_COOKIE=en-US;
TS01bed728=01cc89cf2017a546759944ce232d1f383abee3c2f46805d720c89e52eec641d18361311dfc3b2dbc8d8253766eff5db95f447b2e67;
TS01c25e51=01cc89cf2017a546759944ce232d1f383abee3c2f46805d720c89e52eec641d18361311dfc3b2dbc8d8253766eff5db95f447b2e67
If-None-Match: "4ab22-5b457129962b7"
If-Modified-Since: Wed, 18 Nov 2020 00:55:50 GMT

HTTP/1.1 304 Not Modified
Date: Mon, 23 Nov 2020 14:38:35 GMT
Connection: Keep-Alive
Keep-Alive: timeout=40, max=160
ETag: "4ab22-5b457129962b7"
Expires: Mon, 23 Nov 2020 14:38:36 GMT
Cache-Control: max-age=1
Vary: User-Agent
Set-Cookie: WPID=Q1S1;Path=/;Domain=.bankofamerica.com
Set-Cookie: BOFA_LOCALE_COOKIE=en-US;Path=/;Domain=.bankofamerica.com
X-Serviced-By: /sparta/homepage/--uRewUGTFv5rPMKn1XUTaBQ==--25jWlc7kauzUokhpEPO7TQ==
Strict-Transport-Security: max-age=31536000
Access-Control-Allow-Origin: https://www.bankofamerica.com
Access-Control-Allow-Credentials: true
Access-Control-Max-Age: 3600
Set-Cookie: TS01bed728=01cc89cf2017a546759944ce232d1f383abee3c2f46805d720c89e52eec641d18361311dfc3b2dbc8d8253766eff5db95f447b2e67; Path=/
Set-Cookie: TS01c25e51=01cc89cf2017a546759944ce232d1f383abee3c2f46805d720c89e52eec641d18361311dfc3b2dbc8d8253766eff5db95f447b2e67; path=/; domain=.bankofamerica.com

ICAP/1.0 200 OK
Server: C-ICAP/0.3.5
Connection: keep-alive
ISTag: CI0001-XXXXXXXXX
Encapsulated: res-hdr=0, null-body=999

HTTP/1.1 304 Not Modified
Date: Mon, 23 Nov 2020 14:38:35 GMT
Connection: Keep-Alive
Keep-Alive: timeout=40, max=160
ETag: "4ab22-5b457129962b7"
Expires: Mon, 23 Nov 2020 14:38:36 GMT
Cache-Control: max-age=1
Vary: User-Agent
Set-Cookie: WPID=Q1S1;Path=/;Domain=.bankofamerica.com
Set-Cookie: BOFA_LOCALE_COOKIE=en-US;Path=/;Domain=.bankofamerica.com
X-Serviced-By: /sparta/homepage/--uRewUGTFv5rPMKn1XUTaBQ==--25jWlc7kauzUokhpEPO7TQ==
```

7. Enable the **block** filter for **News** web category:
    - Login to the Alteon
    - Navigate to **Application Delivery → Filters**
    - **Disable** filter **60** (bypass filter from scenario 3)
    - **Enable** filter **70**



Alteon Alteon01

Type: VA (Standalone)
Mgmt IP: 10.100.100.2
HA Status: None
Version: 32.2.3.0
MAC: 00:0C:29:84:15:C6

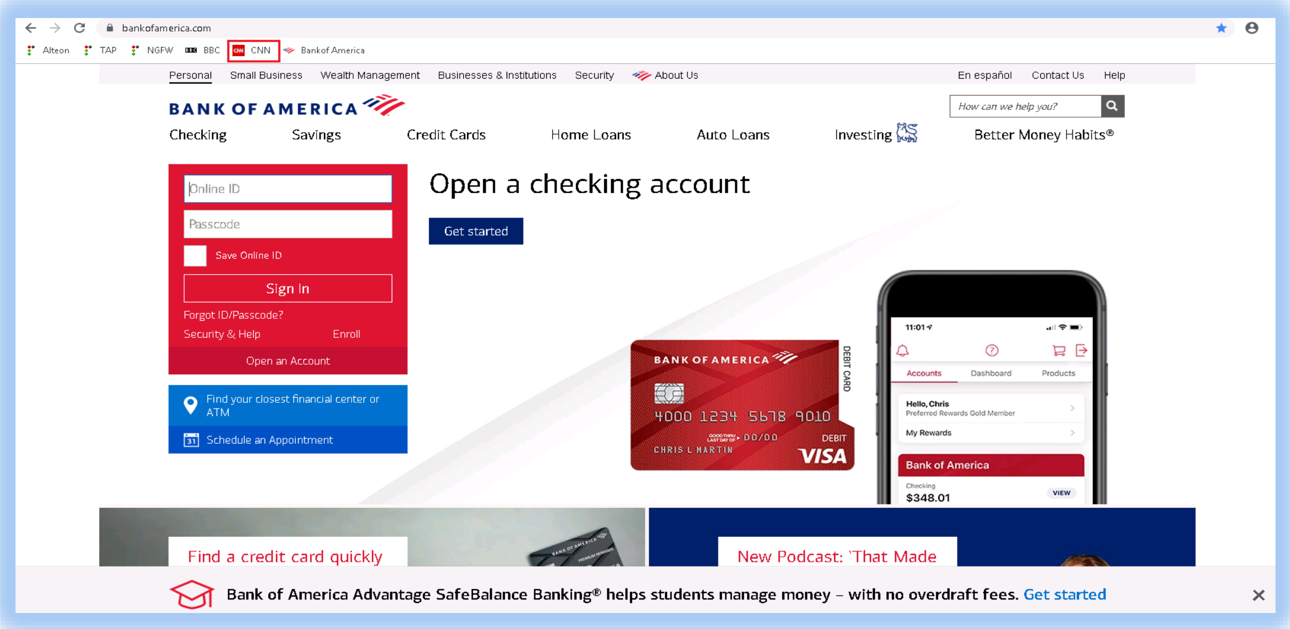
Filters

				Match Settings						
Status	Filter ID	Description	Action	VLAN	Application Port / Range Start	Application Port / Range End	Source IP /Network	Source Mask/Prefix	Destination IP /Network	Destination I
Disabled	50	Bypass BBC.COM	Redirect	Any	443	443	any	0.0.0.0	any	0.0.0.0
Disabled	60	News category bypass	Redirect	Any	443	443	any	0.0.0.0	any	0.0.0.0
Enabled	70	News category block	Deny	Any	443	443	any	0.0.0.0	any	0.0.0.0
Enabled	100	Inspect and send to IDS	Redirect	Any	443	443	any	0.0.0.0	any	0.0.0.0
Enabled	150	Send to IPS	Redirect	Any	81	81	any	0.0.0.0	any	0.0.0.0
Enabled	200	To-GW	Redirect	Any	81	81	any	0.0.0.0	any	0.0.0.0

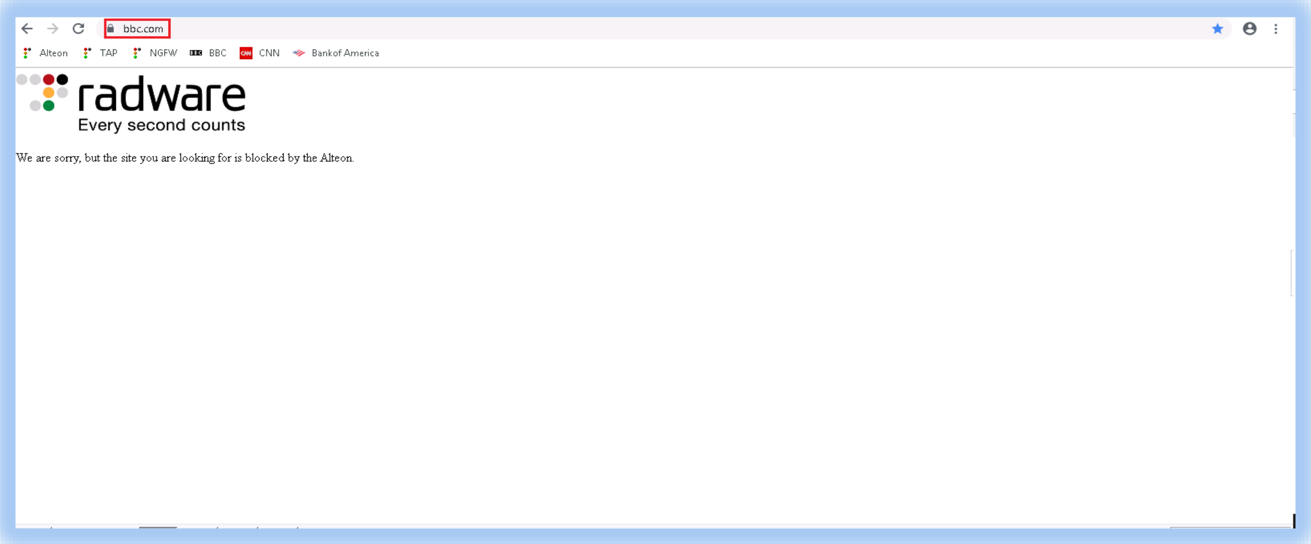
8. Click on **CNN** bookmark:

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided “as is”. Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness or performance



9. The website is **blocked** and we receive a **sorry page**:



We are sorry, but the site you are looking for is blocked by the Alteon.

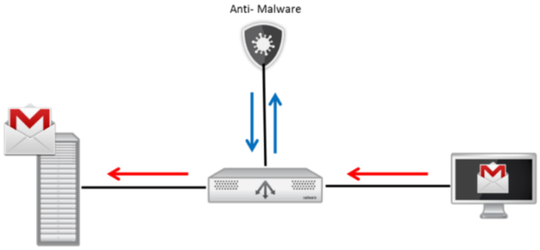
APPENDIX A: SSL INSPECTION OVERVIEW

Radware SSL Inspection solution provides the ability to preserve visibility on organization traffic with the fact that most traffic is encrypted by allowing for transparent decryption of the SSL\TLS traffic in a centralized location.

Key Drivers for Inspecting Outbound SSL Traffic:

- Eliminate blind spots of SSL encrypted communication to/from the enterprise
- Maintaining information's communication's privacy.
- Compliance and regulatory need for information disclosure
  – Log all information access details (what, who when and from where)
  – Prevent unauthorized (source or destination) data communication
- Prevent data leakage of business critical information
- Prevent ingress of malware and advanced persistent threats
  – through SSL encrypted channel
- Monitor traffic to/from cloud applications and services
  – Enforce the organization's data privacy policies on cloud applications as well

SSL Inspection – Deployment Modes



The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

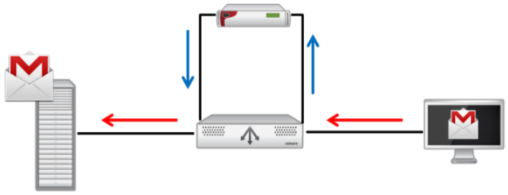
All information provided in the Demo lab and documentation is provided "as is". Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness or performance

Transparent Proxy device

- One leg IPS deployment mode
- Usually used for application level protection
- Anti virus, anti bot, anti malware, WAF
- HTTPS traffic from client is decrypted and forwarded to VAS
- VAS configured in L3 for IPS analysis

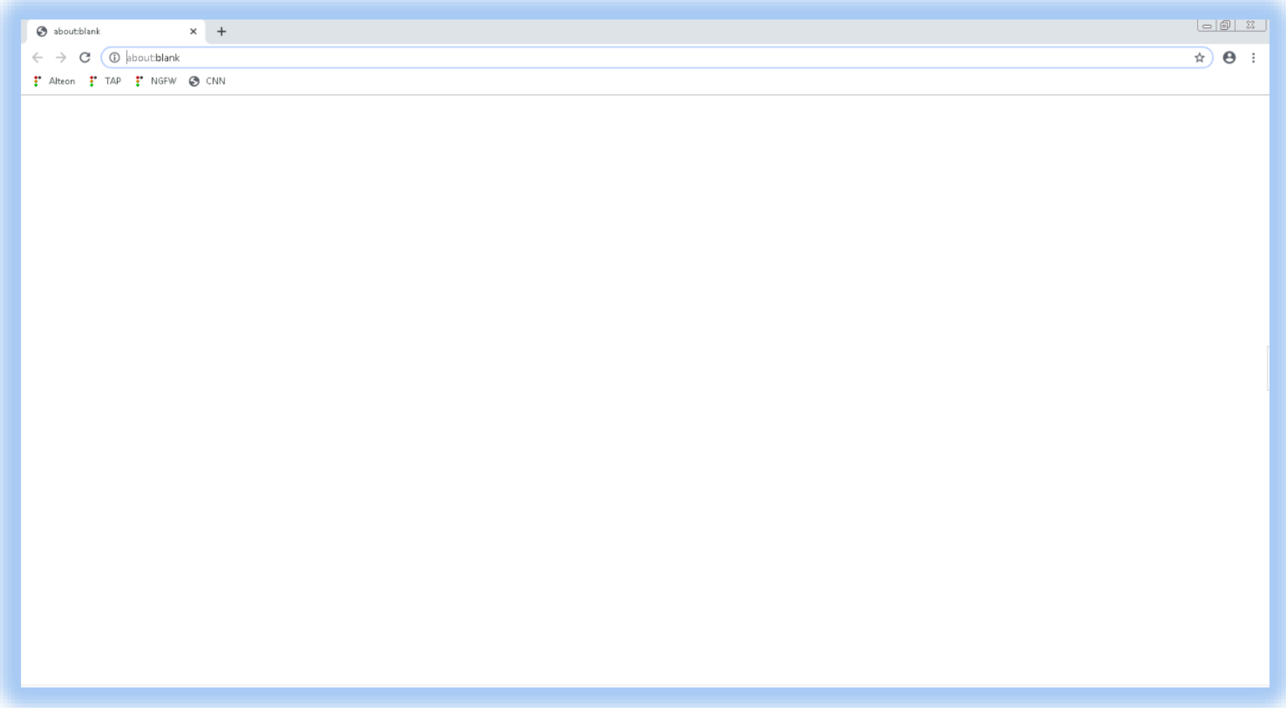
No-MAC (bridge) device

- Two leg IPS deployment mode
- Usually used for network level protection – Anti DDoS
- HTTPS traffic from client is decrypted and forwarded to VAS
- VAS is configured as transparent L2
- (no IP connectivity from Alteon to VAS)

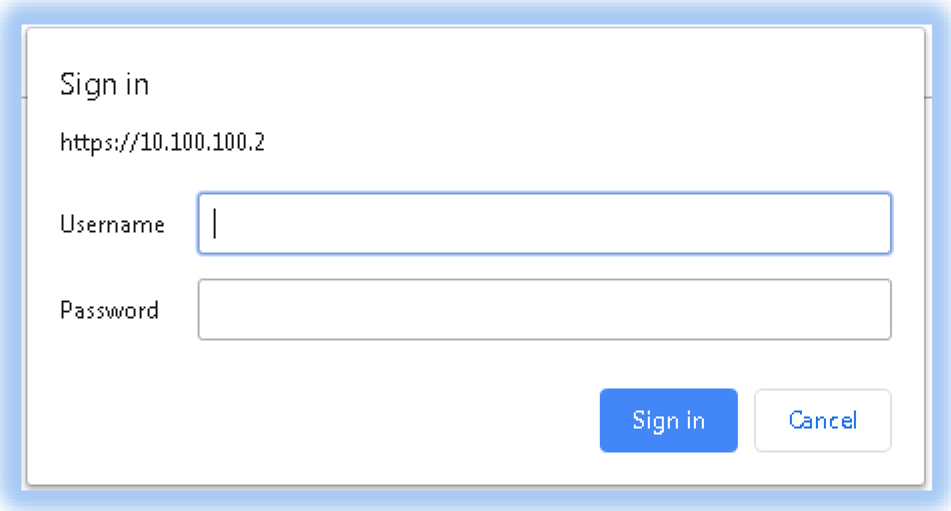


APPENDIX B: IMPORTING ALTEON CONFIGURATION

1. Open Chrome browser and click on the **Alteon** bookmark:



2. Login using credentials **admin/radware**:



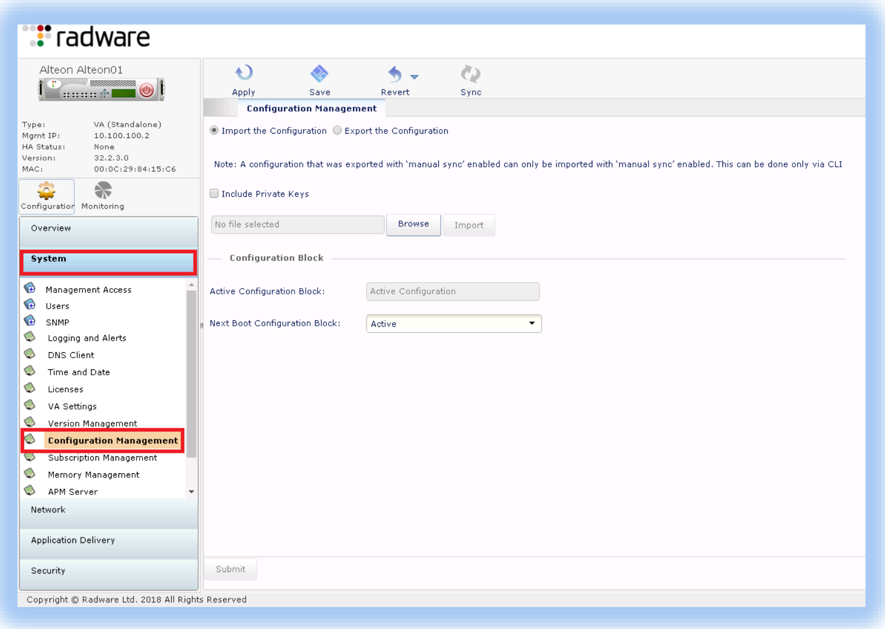
Sign in

https://10.100.100.2

Username

Password

3. Click on **System** and then on **Configuration Management**:



Type: VA (Standalone)
Mgmt IP: 10.100.100.2
HA Status: None
Version: 32.2.3.0
MAC: 00:0C:29:84:15:C6

● Import the Configuration ○ Export the Configuration

Note: A configuration that was exported with 'manual sync' enabled can only be imported with 'manual sync' enabled. This can be done only via CLI

□ Include Private Keys

No file selected

Configuration Block

Active Configuration Block: Active Configuration

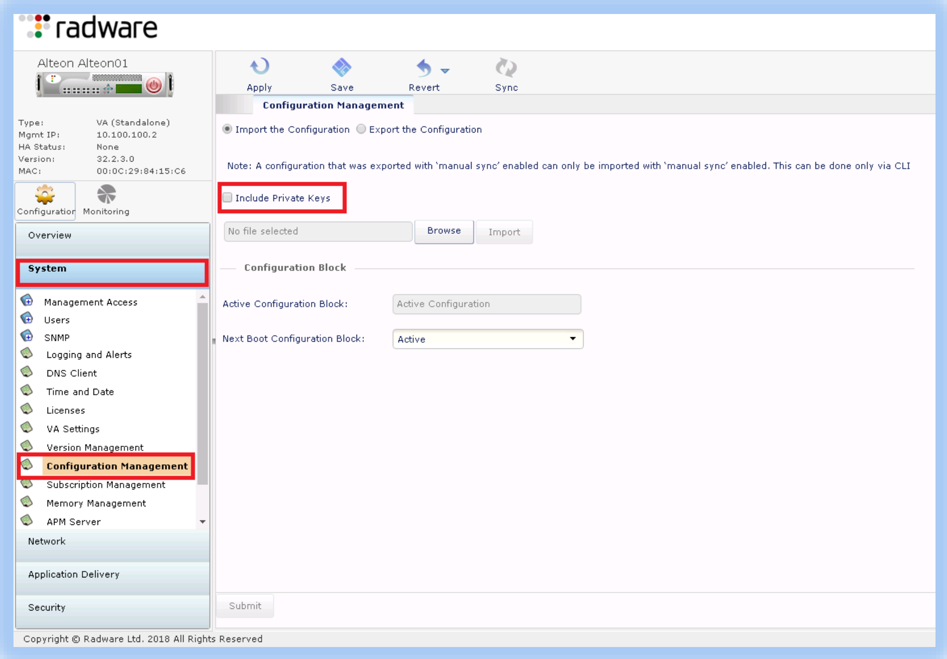
Next Boot Configuration Block: Active

Copyright © Radware Ltd. 2018 All Rights Reserved

4. In the Configuration management screen check **Include Private Keys**, fill the **passphrase** (**radware**) and click **Browse:**

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided "as is". Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness or performance



Type: VA (Standalone)
Mgmt IP: 10.100.100.2
HA Status: None
Version: 32.2.3.0
MAC: 00:0C:29:84:15:C6

● Import the Configuration ○ Export the Configuration

Note: A configuration that was exported with 'manual sync' enabled can only be imported with 'manual sync' enabled. This can be done only via CLI

□ Include Private Keys

No file selected

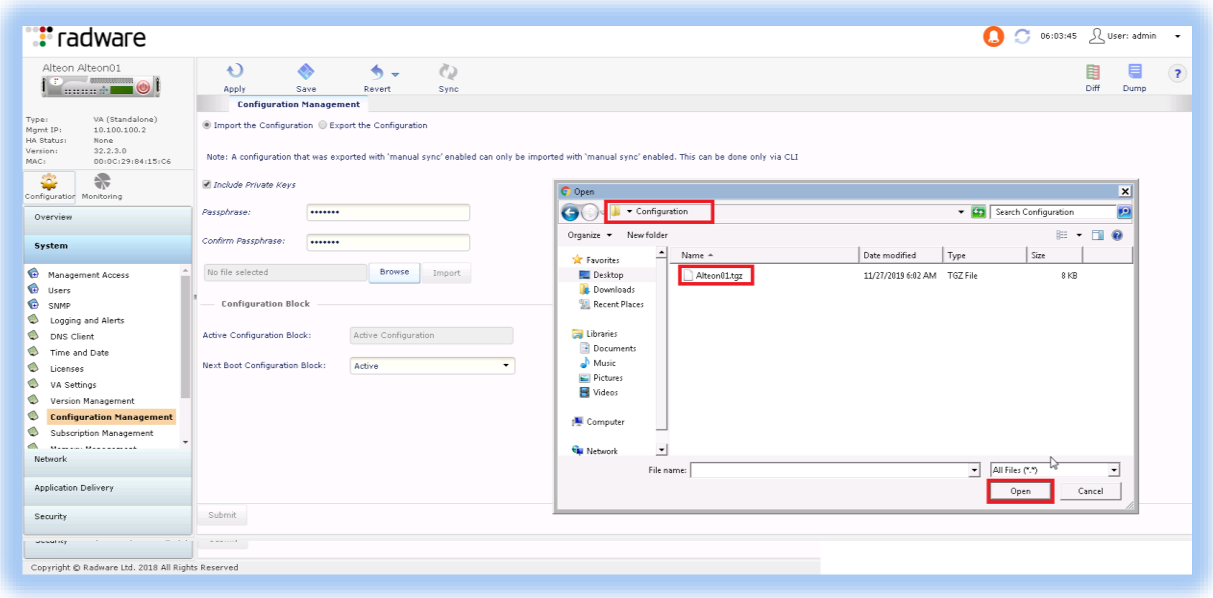
Active Configuration Block: Active Configuration

Next Boot Configuration Block: Active

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided “as is”. Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness or performance

5. Browse to **Documents,** select **Alteon passphrase 1234.tgz**, which contains the default configuration for the SSL Inspection demo then click **Open**:



Type: VA (Standalone)
Mgmt IP: 10.100.100.2
HA Status: None
Version: 32.2.3.0
MAC: 00:0C:29:84:15:C6

● Import the Configuration ○ Export the Configuration

Note: A configuration that was exported with 'manual sync' enabled can only be imported with 'manual sync' enabled. This can be done only via CLI

☑ *Include Private Keys*

Passphrase: •••••••

Confirm Passphrase: •••••••

No file selected

Active Configuration Block: Active Configuration

Next Boot Configuration Block: Active

Configuration

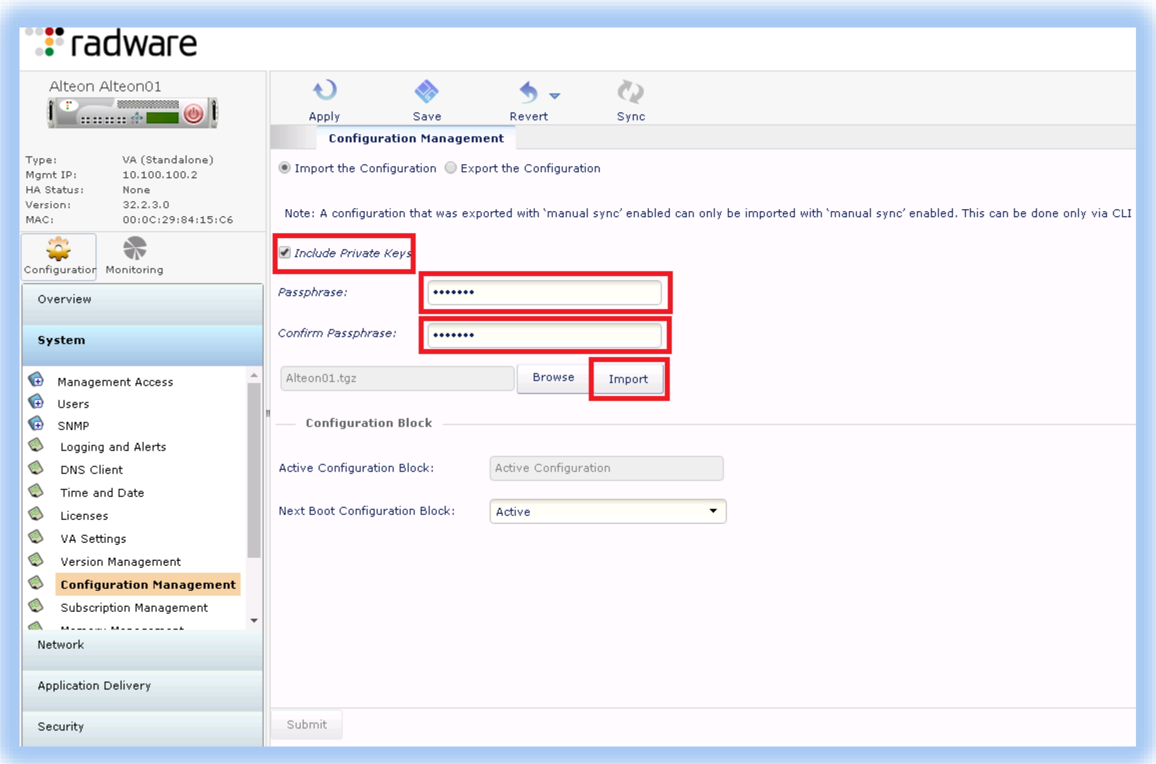
Name	Date modified	Type	Size
Alteon01.tgz	11/27/2019 6:02 AM	TGZ File	8 KB

File name:

All Files (*.*)

Copyright © Radware Ltd. 2018 All Rights Reserved

6. Click **Import** to import the configuration to Alteon.



Alteon Alteon01

Type: VA (Standalone)
Mgmt IP: 10.100.100.2
HA Status: None
Version: 32.2.3.0
MAC: 00:0C:29:84:15:C6

● Import the Configuration ○ Export the Configuration

Note: A configuration that was exported with 'manual sync' enabled can only be imported with 'manual sync' enabled. This can be done only via CLI

☑ Include Private Keys

Passphrase: •••••••

Confirm Passphrase: •••••••

Alteon01.tgz

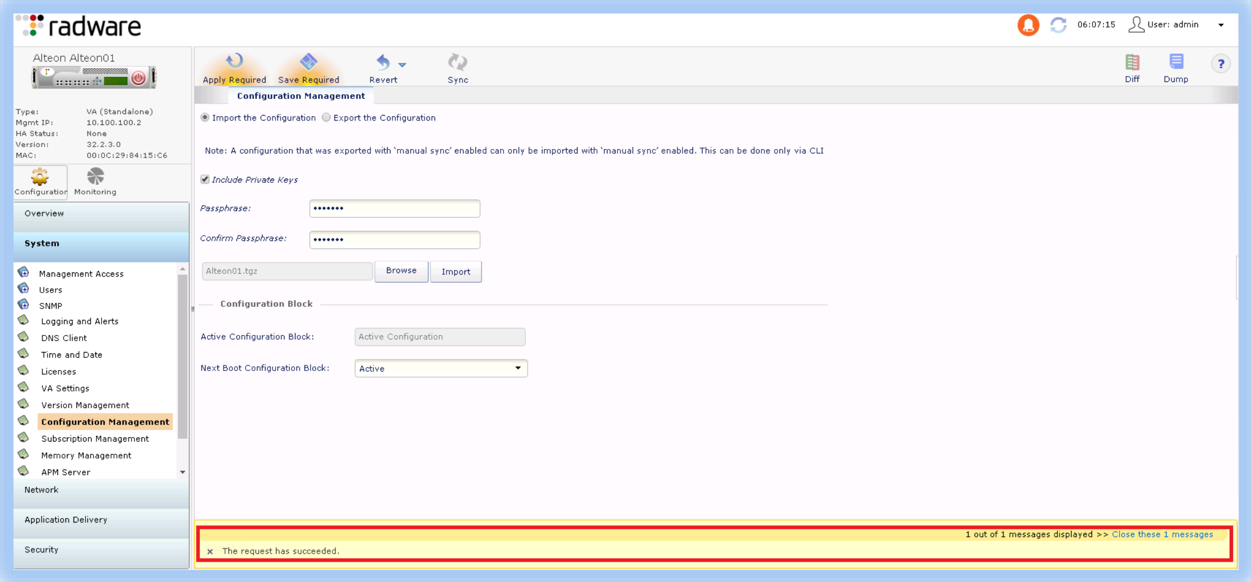
Active Configuration Block: Active Configuration

Next Boot Configuration Block: Active

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided "as is". Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness or performance

7. After the configuration is imported, a message saying **The request has succeeded** displays:



Type: VA (Standalone)
Mgmt IP: 10.100.100.2
HA Status: None
Version: 32.2.3.0
MAC: 00:0C:29:84:15:C6

● Import the Configuration ○ Export the Configuration

Note: A configuration that was exported with 'manual sync' enabled can only be imported with 'manual sync' enabled. This can be done only via CLI

☑ *Include Private Keys*

Passphrase: •••••••

Confirm Passphrase: •••••••

Alteon01.tgz

Active Configuration Block: Active Configuration

Next Boot Configuration Block: Active

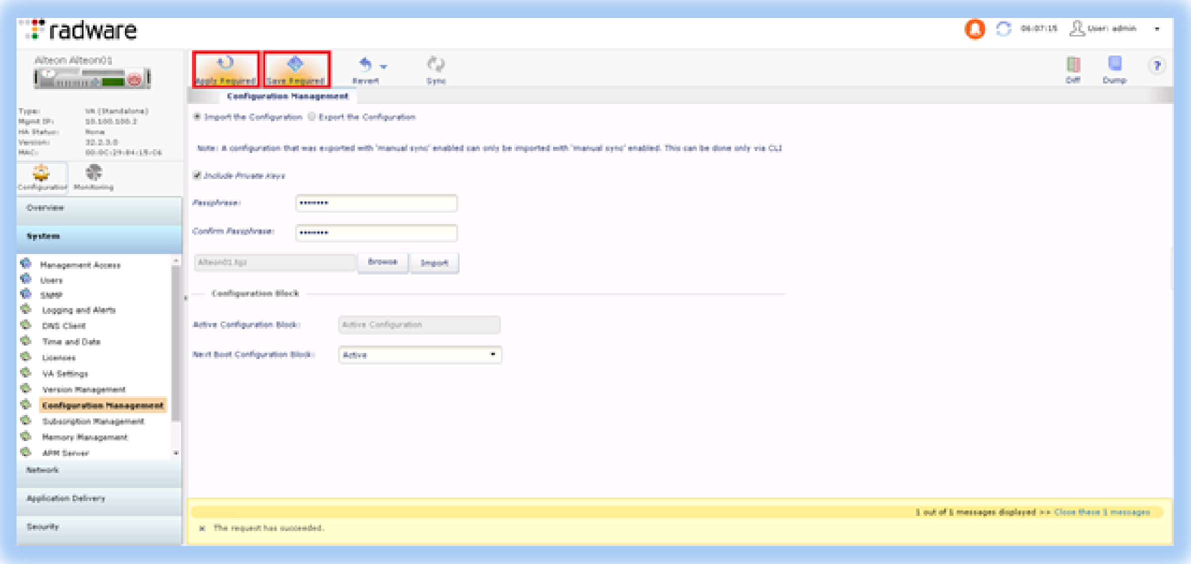
1 out of 1 messages displayed >> Close these 1 messages

× The request has succeeded.

8. Click **Apply**" button to apply the configuration and "Save" for save it on boot config:

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided "as is". Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness or performance



Type: VA (Standalone)
Mgmt IP: 10.100.100.2
HA Status: None
Version: 32.2.3.0
MAC: 00:0C:29:84:15:C6

Configuration Management

● Import the Configuration ○ Export the Configuration

Note: A configuration that was exported with 'manual sync' enabled can only be imported with 'manual sync' enabled. This can be done only via CLI

☑ Include Private Keys

Passphrase: ••••••••

Confirm Passphrase: ••••••••

Alteon01.tgz

Configuration Block

Active Configuration Block: Active Configuration

Next Boot Configuration Block: Active

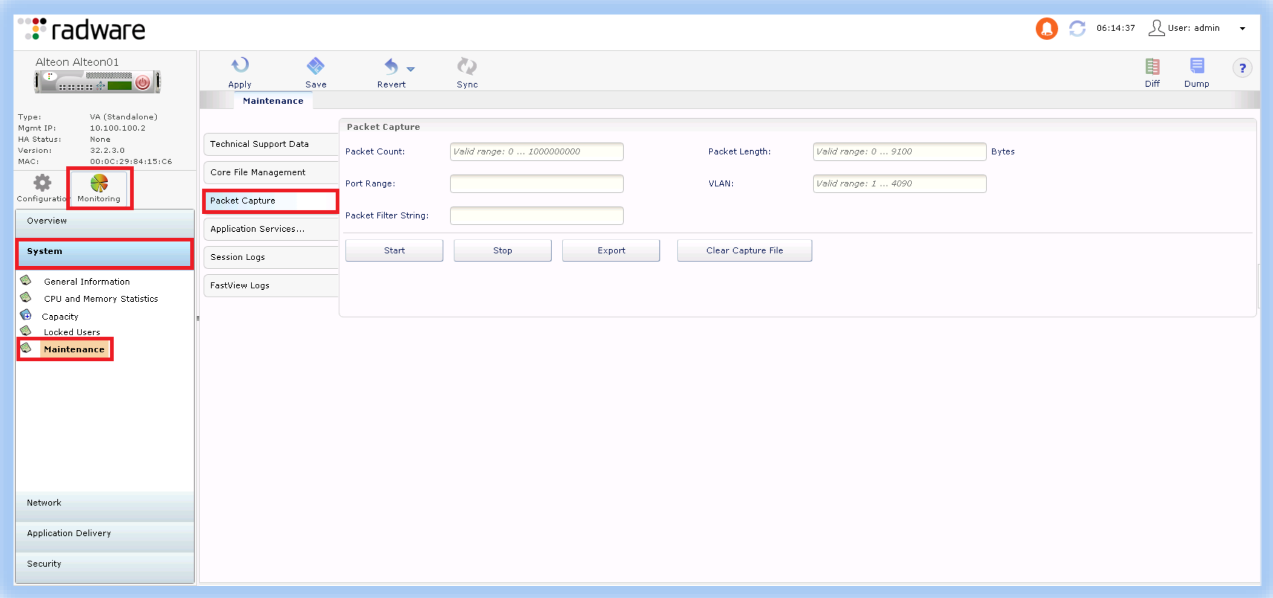
The request has succeeded.

APPENDIX C: RUNNING PACKET CAPTURES

You can use packet captures on the Alteon in order to show the traffic flow through different security devices. Since the redirection is done in L2 you should look at the MAC addresses in order to understand the packets source and destination.

To run the capture on the Alteon perform the following:

1. On the Alteon main screen – Click on: **Monitoring → System → Maintenance → Packet Capture**:

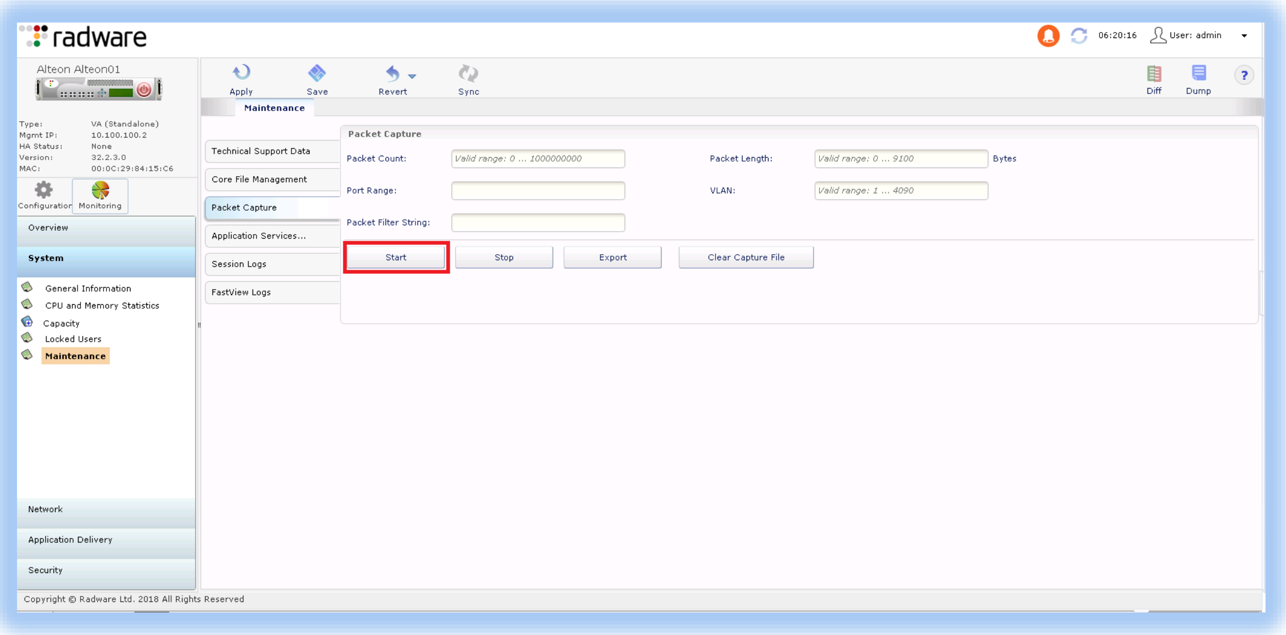


Type:	VA (Standalone)
Mgmt IP:	10.100.100.2
HA Status:	None
Version:	32.2.3.0
MAC:	00:0C:29:84:15:C6

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided “as is”. Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness or performance

2. Click on **Start** to start packet capture:



Alteon Alteon01

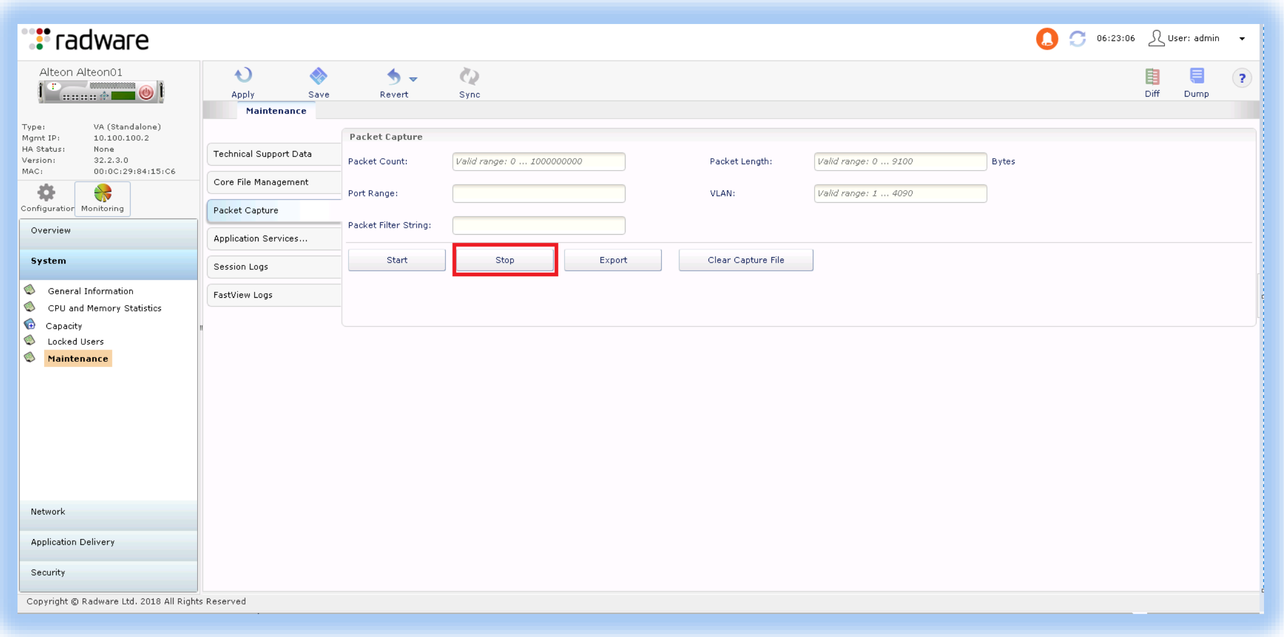
Type: VA (Standalone)
Mgmt IP: 10.100.100.2
HA Status: None
Version: 32.2.3.0
MAC: 00:0C:29:84:15:C6

Packet Capture

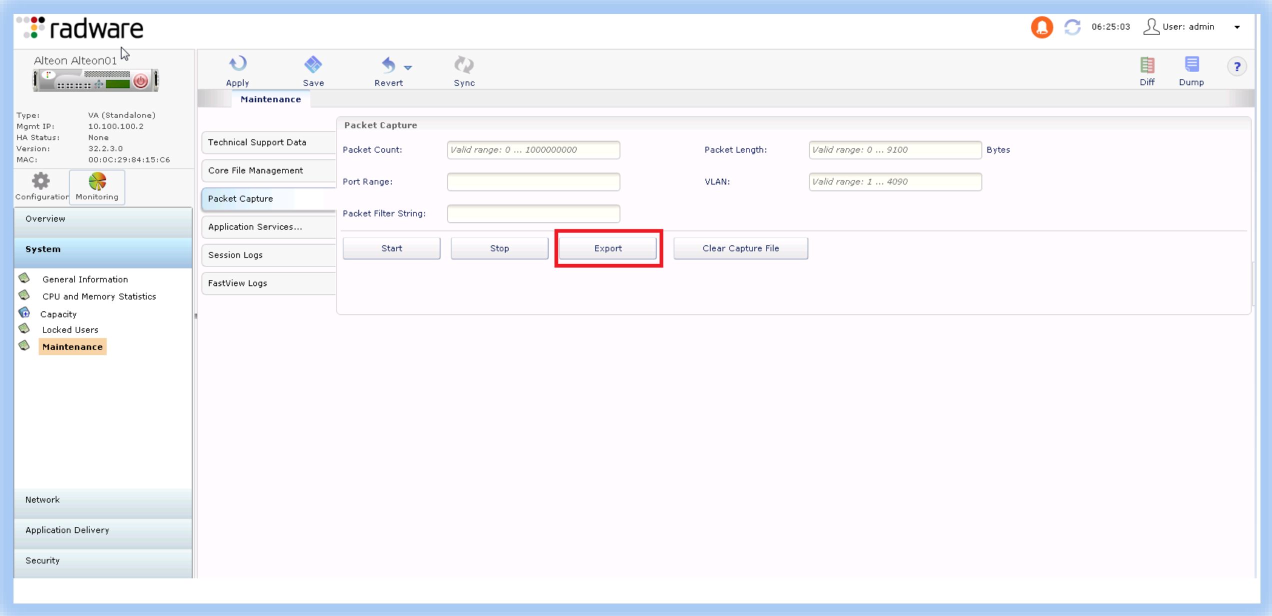
Packet Count: Valid range: 0 ... 1000000000
Packet Length: Valid range: 0 ... 9100 Bytes
Port Range:
VLAN: Valid range: 1 ... 4090
Packet Filter String:

Copyright © Radware Ltd. 2018 All Rights Reserved

3. Run the traffic through the Alteon
4. Click on **Stop** to stop packet capture:



Type: VA (Standalone)
Mgmt IP: 10.100.100.2
HA Status: None
Version: 32.2.3.0
MAC: 00:0C:29:84:15:C6



Type: VA (Standalone)
Mgmt IP: 10.100.100.2
HA Status: None
Version: 32.2.3.0
MAC: 00:0C:29:84:15:C6

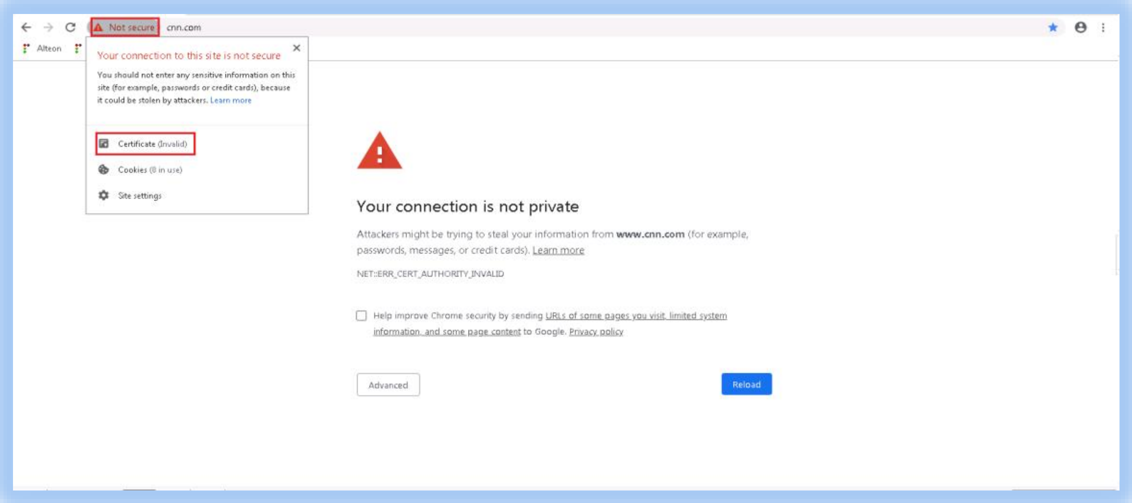
Packet Count: Valid range: 0 ... 1000000000
Packet Length: Valid range: 0 ... 9100 Bytes
Port Range:
VLAN: Valid range: 1 ... 4090
Packet Filter String:

5. Click on **Export** to export PCAP file:

6. Open the capture file in WireShark and inspect the flow based on MAC address changes.

APPENDIX D: ADDING THE ALTEON AS A TRUSTED CA

1. When you first receive the Alteon issued certificate you will receive an error. Click on **Not secure** for more information, then click on **Certificate (Invalid)**:



Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more

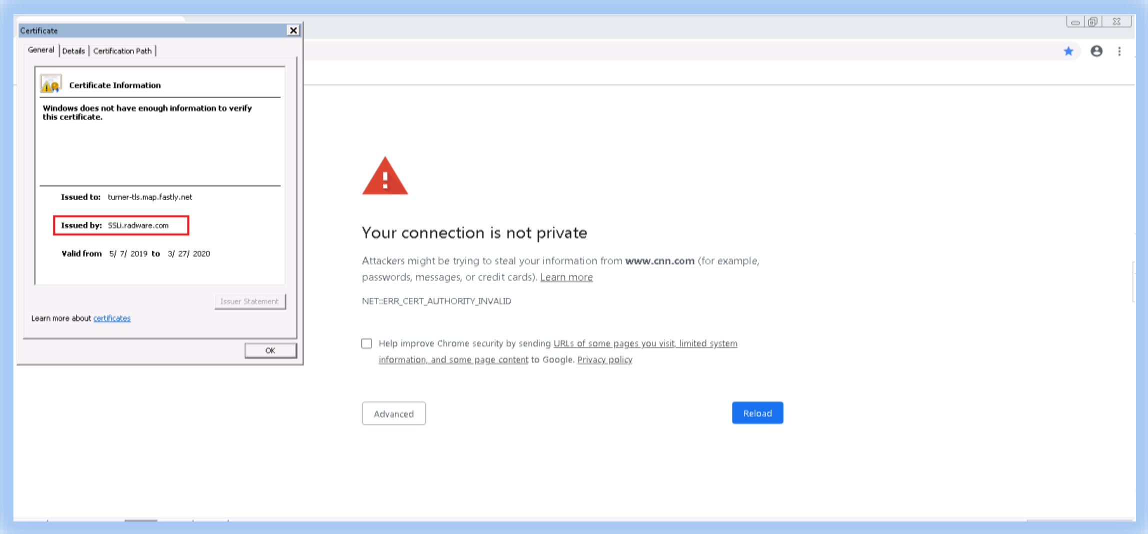
Your connection is not private

Attackers might be trying to steal your information from **www.cnn.com** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

□ Help improve Chrome security by sending URLs of some pages you visit, limited system information, and some page content to Google. Privacy policy

2. We can see that the Alteon issued certificate is not trusted by the PC:



Windows does not have enough information to verify this certificate.

Issued to: turner-tls.map.fastly.net

Issued by: SSLi.radware.com

Valid from 5/ 7/ 2019 **to** 3/ 27/ 2020

Learn more about certificates

Your connection is not private

Attackers might be trying to steal your information from **www.cnn.com** (for example, passwords, messages, or credit cards). Learn more

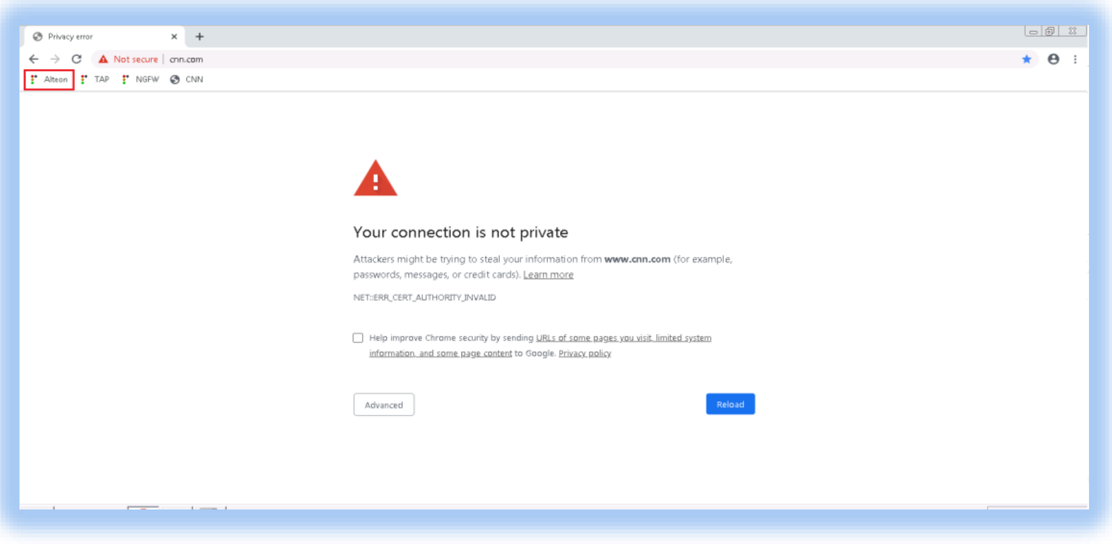
NET::ERR_CERT_AUTHORITY_INVALID

□ Help improve Chrome security by sending URLs of some pages you visit, limited system information, and some page content to Google. Privacy policy

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided “as is”. Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness or performance

3. In order to trust the certificate browse to the **Alteon** and **login**:



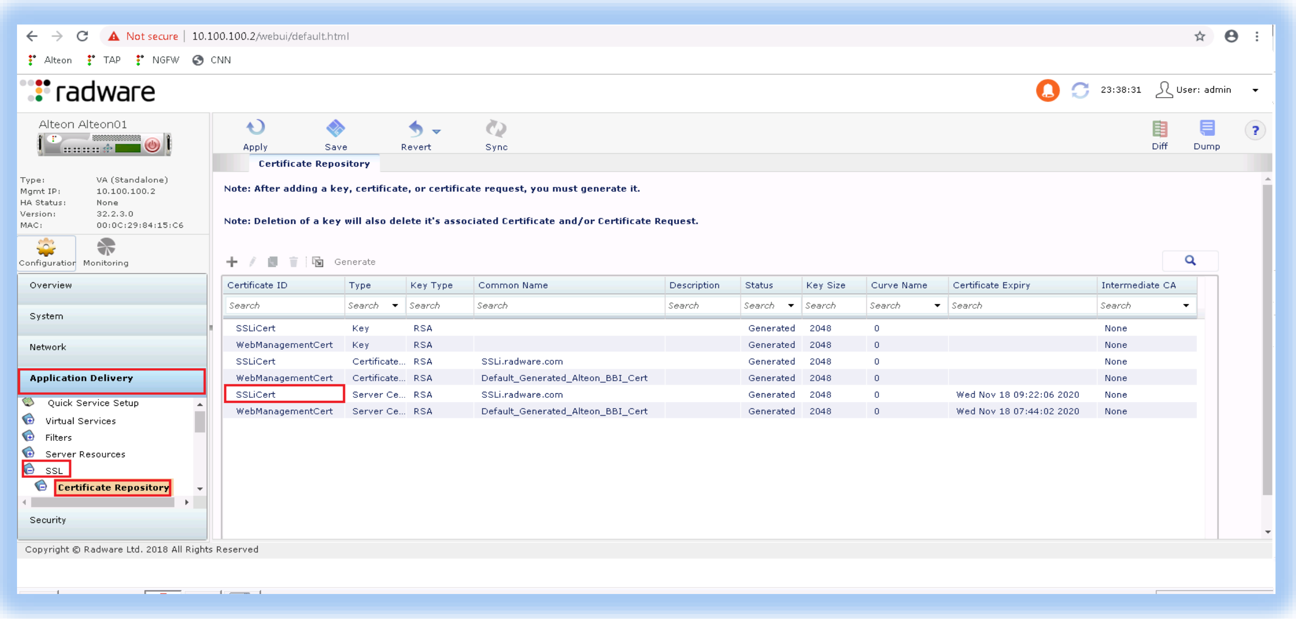
Your connection is not private

Attackers might be trying to steal your information from **www.cnn.com** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

□ Help improve Chrome security by sending URLs of some pages you visit, limited system information, and some page content to Google. Privacy policy

4. Navigate to **Application Delivery → SSL → Certificate Repository** then double click on **SSLiCert**:



Type: VA (Standalone)
Mgmt IP: 10.100.100.2
HA Status: None
Version: 32.2.3.0
MAC: 00:0C:29:84:15:C6

Note: After adding a key, certificate, or certificate request, you must generate it.

Note: Deletion of a key will also delete it's associated Certificate and/or Certificate Request.

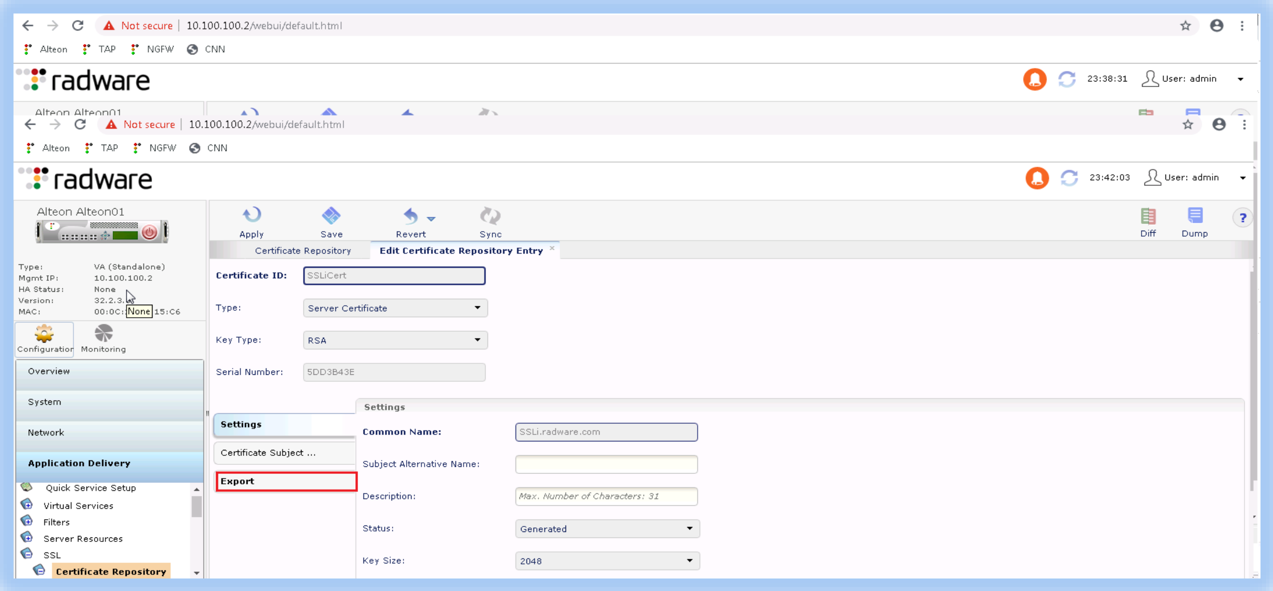
Certificate ID	Type	Key Type	Common Name	Description	Status	Key Size	Curve Name	Certificate Expiry	Intermediate CA
Search	Search	Search	Search	Search	Search	Search	Search	Search	Search
SSLiCert	Key	RSA			Generated	2048	0		None
WebManagementCert	Key	RSA			Generated	2048	0		None
SSLiCert	Certificate...	RSA	SSLi.radware.com		Generated	2048	0		None
WebManagementCert	Certificate...	RSA	Default_Generated_Alteon_BBI_Cert		Generated	2048	0		None
SSLiCert	Server Ce...	RSA	SSLi.radware.com		Generated	2048	0	Wed Nov 18 09:22:06 2020	None
WebManagementCert	Server Ce...	RSA	Default_Generated_Alteon_BBI_Cert		Generated	2048	0	Wed Nov 18 07:44:02 2020	None

Copyright © Radware Ltd. 2018 All Rights Reserved

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided "as is". Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness or performance

5. Click on **Export**:

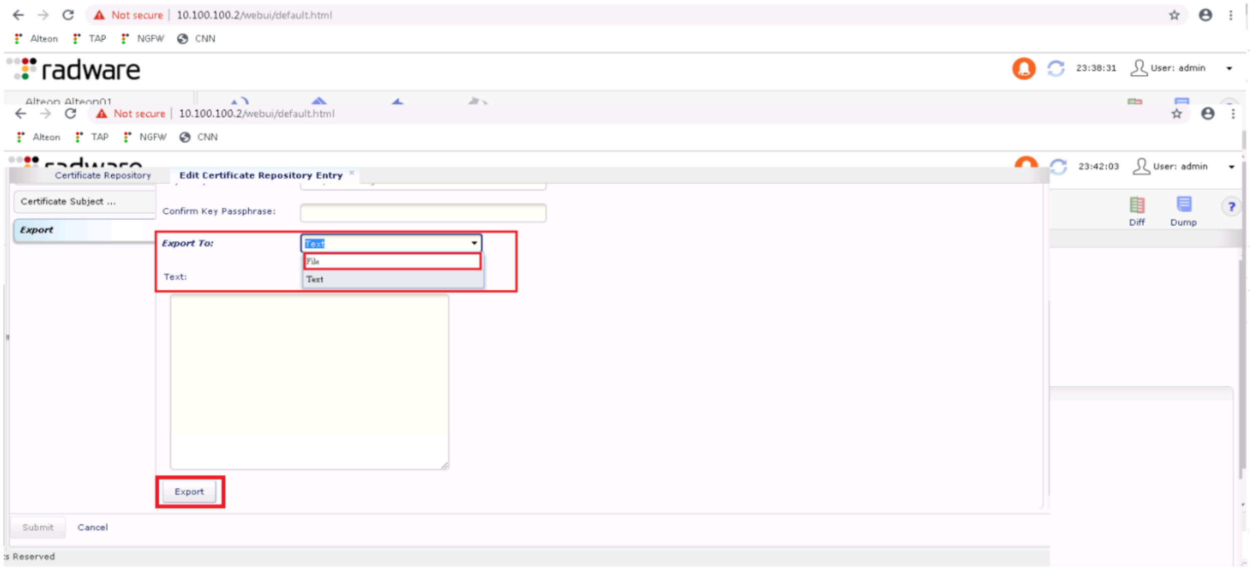


Type: VA (Standalone)
Mgmt IP: 10.100.100.2
HA Status: None
Version: 32.2.3.
MAC: 00:0C: 15:C6

Certificate ID: SSLiCert
Type: Server Certificate
Key Type: RSA
Serial Number: 5DD3B43E

Settings
Common Name: SSLi.radware.com
Subject Alternative Name:
Description: Max. Number of Characters: 31
Status: Generated
Key Size: 2048

6. Select **Export to: File** and click **Export** in order to download the certificate:

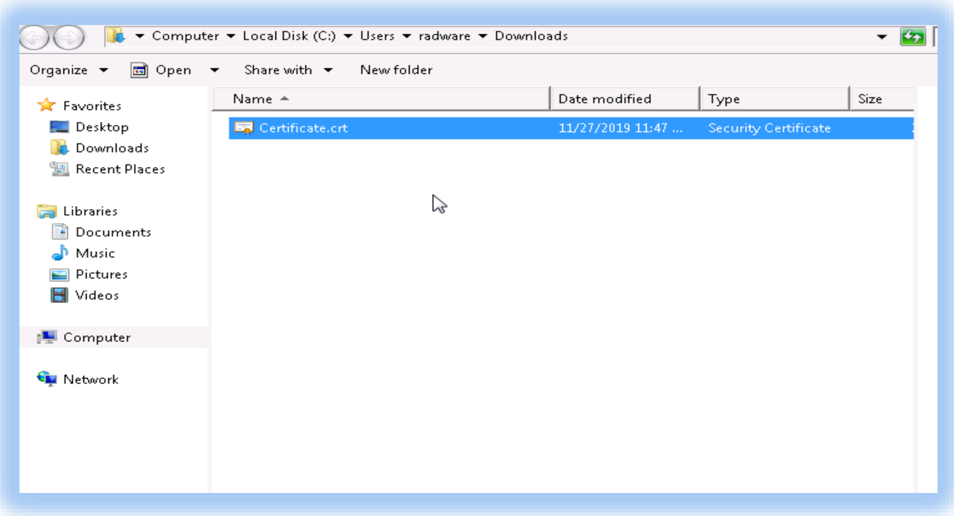


Confirm Key Passphrase:
Export To: Text
Text:

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

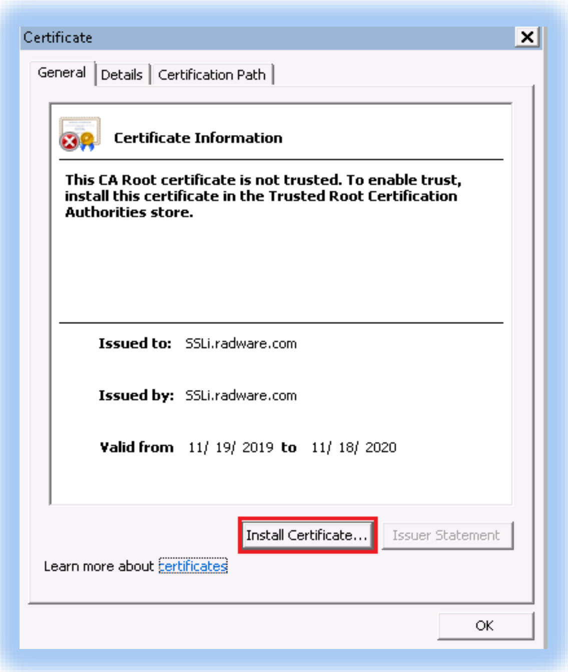
All information provided in the Demo lab and documentation is provided “as is”. Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness or performance

7. Browse to the certificate location and change its extension from **.txt** to **.crt**



Name	Date modified	Type	Size
Certificate.crt	11/27/2019 11:47 ...	Security Certificate	

8. Double click the certificate to open it and click on **Install Certificate**



Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: SSLi.radware.com

Issued by: SSLi.radware.com

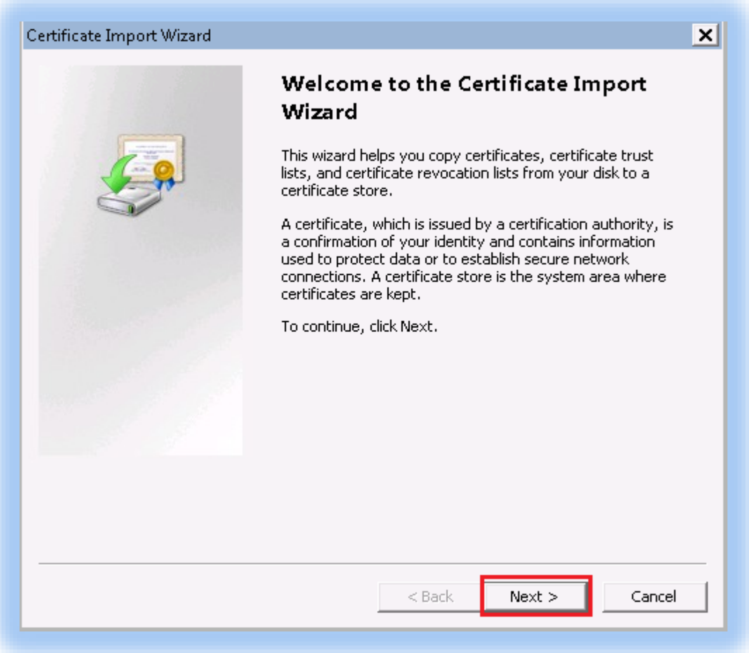
Valid from 11/ 19/ 2019 **to** 11/ 18/ 2020

Learn more about certificates

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided “as is”. Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness or performance

9. The Certificate Import Wizard will open. Click **Next** to proceed:



Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

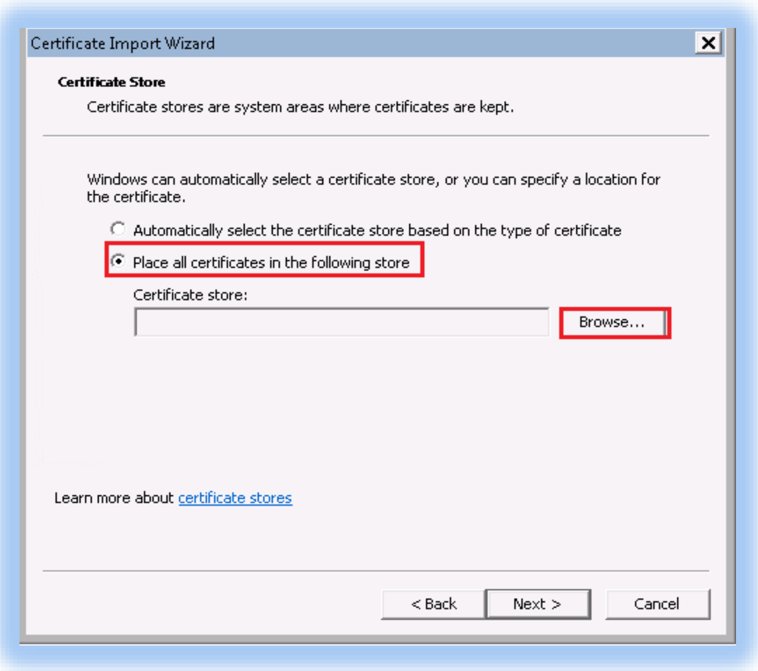
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

10. Select **Place all certificates in the following store** and click **Browse**:

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided “as is”. Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness or performance



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

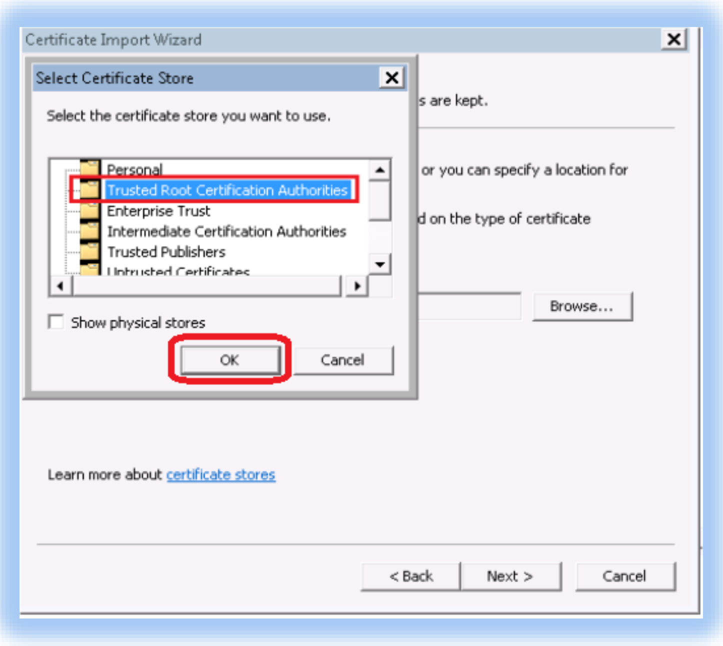
● Place all certificates in the following store

Certificate store:

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided “as is”. Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness or performance

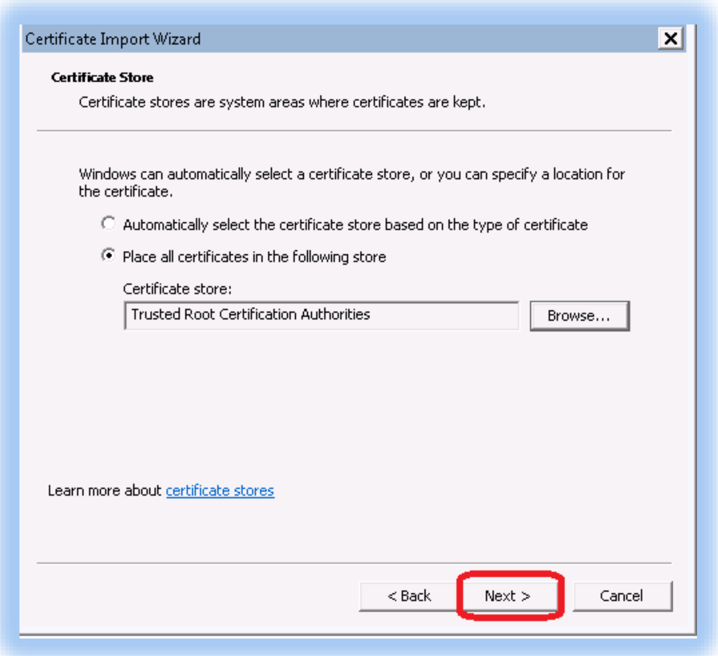
11. Choose **Trusted Root Certificate Authorities** and click **OK**:



Select the certificate store you want to use.

Certificate Import Wizard
Select Certificate Store
Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Show physical stores
OK
Cancel
s are kept.
or you can specify a location for
d on the type of certificate
Browse...
Learn more about certificate stores
< Back
Next >
Cancel

12. Click **Next** to import the certificate:



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

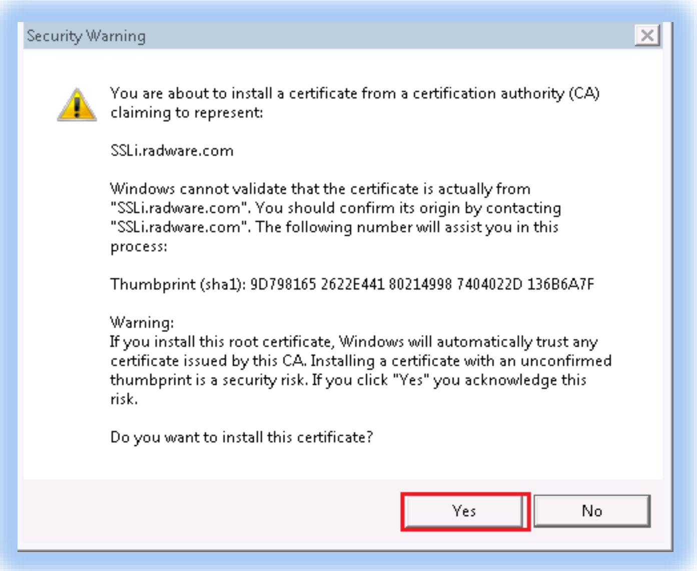
● Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

Learn more about certificate stores

13. Click **Yes** to confirm you trust this certificate and install it:



Security Warning

You are about to install a certificate from a certification authority (CA) claiming to represent:

SSLi.radware.com

Windows cannot validate that the certificate is actually from "SSLi.radware.com". You should confirm its origin by contacting "SSLi.radware.com". The following number will assist you in this process:

Thumbprint (sha1): 9D798165 2622E441 80214998 7404022D 136B6A7F

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided “as is”. Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness or performance

APPENDIX E: SCENARIO 1 CONFIGURATION

All the traffic passes through the Alteon and the SSL inspection is performed using 3 filters: 100,150,200.

1. ***Filter 100***

Description:

Intercepts SSL traffic from the client and sends clear traffic to the ICAP server and the IDS on port 81.

Classification:

- Destination TCP port 443.
- Source interface 1 (client side).

Action:

- Perform SSL negotiation with the client in order to decrypt the request.
- Send a copy of the decrypted traffic to the IDS server on port 81.
- Send the decrypted traffic to the ICAP server on port 81.

Configuration:

```
/c/slb/port "1"
    filt ena
    add 100
 /c/slb/filt 100
    name "Inspect and send to IDS"
    ena
    action redir
    proto tcp
    dport https
    group IDS
    rport 81
    add 1
    applic http
```

```
/c/slb/filt 100/ssl
    sslpol FESSLPolicy
    inspect ena
    l7action inspect
/c/slb/filt 100/adv
    icap icap_policy
    thash sip
    rtsrcmac ena
    reverse ena
/c/slb/filt 100/adv/redir
    dbind forceproxy
    fallback continueFlow
    fbport 4
/c/slb/filt 100/report/inspect
    ena
    location clientside
    purpose inspect
    app https
    dir outbound
```

2.

Filter 150

Description:

Intercept HTTP traffic returning from the ICAP server and send it to the NGFW server.

Classification:

- Destination TCP port 81
- Source interface 3 (ICAP server)

Action:

- Send the traffic to the NGFW server

Configuration:

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided “as is”. Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness or performance

```
    /c/slb/filt 150
        name "Send to NGFW"
        ena
        action redir
        proto tcp
        dport 81
        group NGFW
        rport 81
        add 2
    /c/slb/filt 150/adv
        rtsrcmac ena
        reverse ena
    /c/slb/filt 150/adv/redir
        fallback continueFlow
        fbport 4
/c/slb/filt 150/report/inspect
    ena
    location clientside
    purpose inspect
    app https
    dir outbound
```

3. *Filter 200*

Description:

Intercept HTTP traffic returning from the NGFW server, re-encrypt it and send it to the internet.

Classification:

- Destination TCP port 81

The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided “as is”. Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness or performance

- Source interface 5 (NGFW server)

Action:

- Re-encrypt the traffic.
- Send the encrypted traffic to the default gateway on port 443

Configuration:

```
/c/slb/port "4"
    filt ena
    add 200
/c/slb/filt 200
    name "To-GW"
    ena
    action redir
    proto tcp
    dport 81
    group GW
    rport 443
    add 4
    applic http
/c/slb/filt 200/ssl
    sslpol BESSLPolicy
    inspect ena
/c/slb/filt 200/adv
    matchdev all
    rtsrcmac ena
    reverse ena
/c/slb/filt 200/adv/proxyadv
    proxyip 192.168.200.253
/c/slb/filt 200/adv/redir
    dbind forceproxy
   /c/slb/filt 200/report/inspect
    ena
    location serverside
    purpose inspect
    app https
    dir outbound
```

APPENDIX F: SCENARIO 2 CONFIGURATION

Description:

Filter 50 is configured to bypass SSL inspection for requests to host www.bbc.com and send them directly to the internet.

Classification:

- Destination TCP port 443.
- Source interface 1 (Clients side).
- Host name www.bbc.com.

Action:

- Send the traffic to directly to the default gateway.

Configuration

```
/c/slb/port "1"
    add 50

/c/slb/layer7/slb
/c/slb/layer7/slb/cntclss Host_Bypass ssl
/c/slb/layer7/slb/cntclss Host_Bypass ssl/hostname www.bbc.com
    hostname "www.bbc.com"
/c/slb/filt 50
    name "Bypass bbc.COM"
    ena
    action redir
    ipver v4
    sip any
    smask 0.0.0.0
    dip any
    dmask 0.0.0.0
    proto tcp
    dport https
```

```
     group GW
     rport 443
     vlan any
     add 1
     cntclss Host_Bypass
     applic http
 /c/slb/filt 50/ssl
     sslpol Outbound_FE_SSL_Inspection
     inspect ena
     l7action bypass
 /c/slb/filt 50/adv
     rtsrcmac ena
     reverse ena
 /c/slb/filt 50/adv/proxyadv
     proxyip 192.168.200.253
 /c/slb/filt 50/adv/redir
     dbind forceproxy
/c/slb/filt 50/report/inspect
     ena
     location clientside
     purpose bypass
     app https
     dir outbound
```

APPENDIX G: SCENARIO 3 CONFIGURATION

Description:

Filter 60 is configured to bypass SSL inspection for requests to any NEWS site and send them directly to the internet.

Classification:

- Destination TCP port 443.
- Source interface 1 (Clients side).
- Host name matches NEWS category.

Action:

Send the traffic to directly to the default gateway

Configuration:

```
/c/slb/layer7/urlfiltr/urlpol News_Bypass
/c/slb/layer7/urlfiltr/urlpol News_Bypass/categs/prod
    42
/c/slb/port "1"
    add 60
/c/slb/filt 60
    name "News category bypass"
    ena
    action redir
    ipver v4
    sip any
    smask 0.0.0.0
    dip any
    dmask 0.0.0.0
    proto tcp
    dport https
    group GW
    rport 443
    vlan any
    add 1
    urlfilt News_Bypass
    applic http
 /c/slb/filt 60/ssl
```

```
     sslpol Outbound_FE_SSL_Inspection
     inspect ena
     l7action bypass
/c/slb/filt 60/adv
     rtsrcmac ena
     reverse ena
/c/slb/filt 60/adv/proxyadv
     proxyip 192.168.200.253
/c/slb/filt 60/adv/redir
     dbind forceproxy
/c/slb/filt 60/report/inspect
     ena
     location clientside
     purpose bypass
     app https
     dir outbound
```

APPENDIX H: SCENARIO 4 CONFIGURATION

Description:

Filter 70 is configured to block requests to any NEWS site and present the client with a sorry page.

Classification:

- Destination TCP port 443.
- Source interface 1 (Clients side).
- Host name matches NEWS category.

Action:

Block the traffic and display sorry page.

Configuration

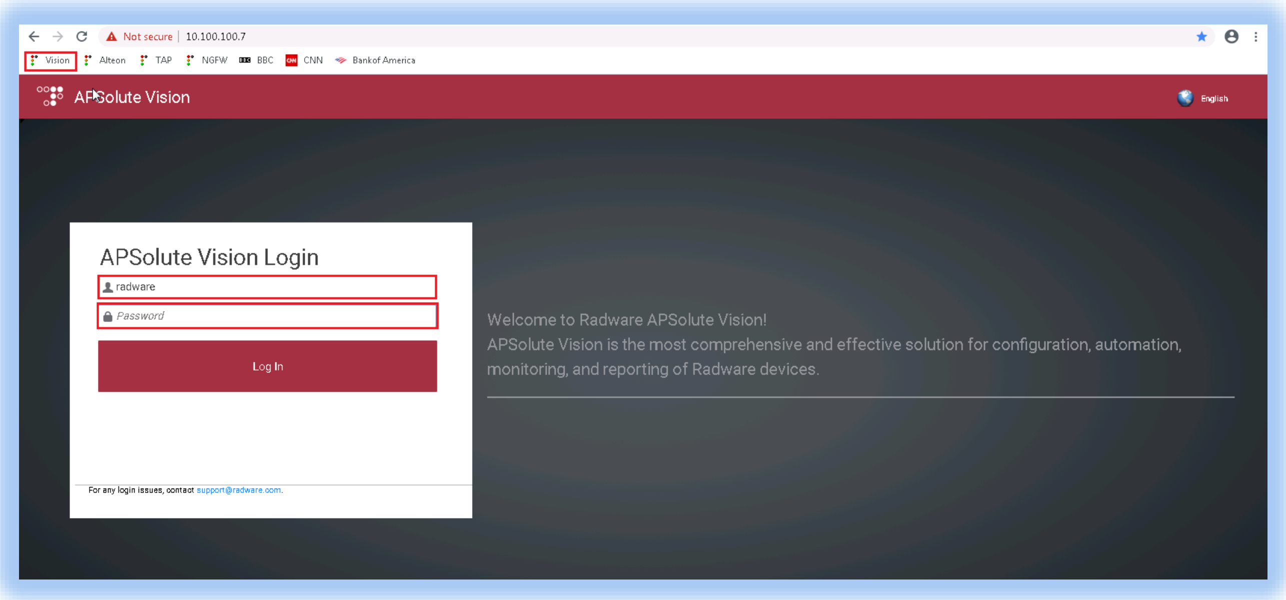
```
/c/slb/appshape/script SorryPage
    ena
    import text
 when HTTP_REQUEST {
   if { [HTTP::method]   ne "HEAD" } {
 HTTP::respond 200 content {
     <html>
       <p><img src="https://www.israel-
braingain.org.il/uploads/images/small_16457.jpg" alt="" width="286" height="78"
/>&nbsp;</p>
 <p>We are sorry, but the site you are looking for is blocked by the Alteon.</p>
     </html>
 }
 }
 }
 -----END

 /c/slb/port "1"
    add 70

 /c/slb/filt 70
```

```
     name "News category block"
     ena
     action redir
     ipver v4
     sip any
     smask 0.0.0.0
     dip any
     dmask 0.0.0.0
     proto tcp
     dport https
     group IDS
     rport 81
     vlan any
     add 1
     urlfilt News_Bypass
     applic http
 /c/slb/filt 70/ssl
     sslpol FESSLPolicy
     inspect ena
     l7action inspect
 /c/slb/filt 70/adv
     rtsrcmac ena
 /c/slb/filt 70/adv/redir
     dbind forceproxy
     fallback continueFlow
     fbport 4
 /c/slb/filt 70/appshape/add 1 SorryPage
/c/slb/filt 70/report/inspect
     ena
     location clientside
     purpose bypass
     app https
     dir outbound
```

APPENDIX I: VISION SSL INSPECTION ANALYTICS

In order to view SSL Inspection dashboard on Vision, please refer the following steps:

1. Click on Vision tab (U/P radware/radware):



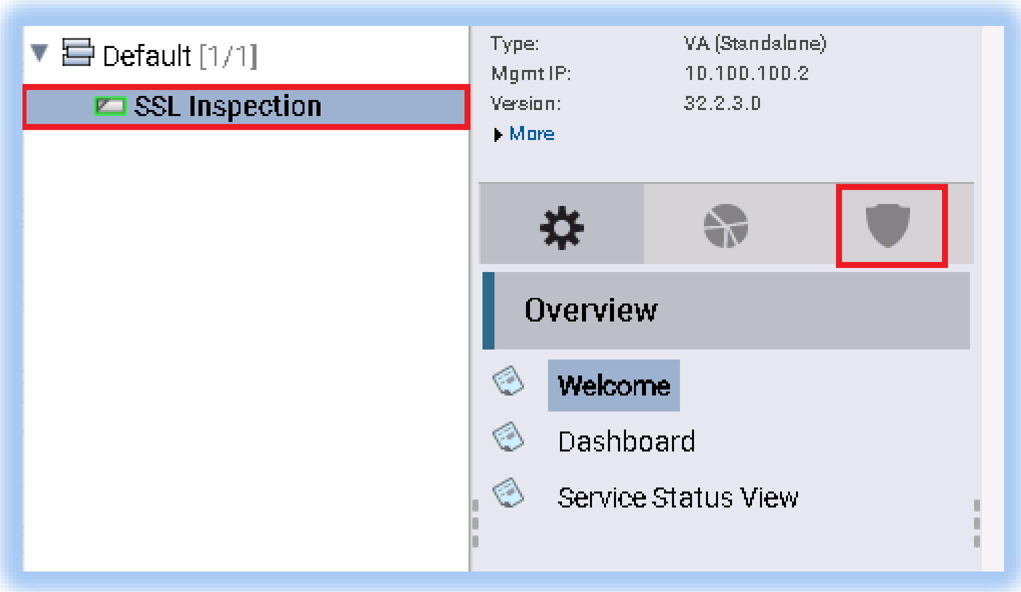
APSolute Vision Login

radware

Password

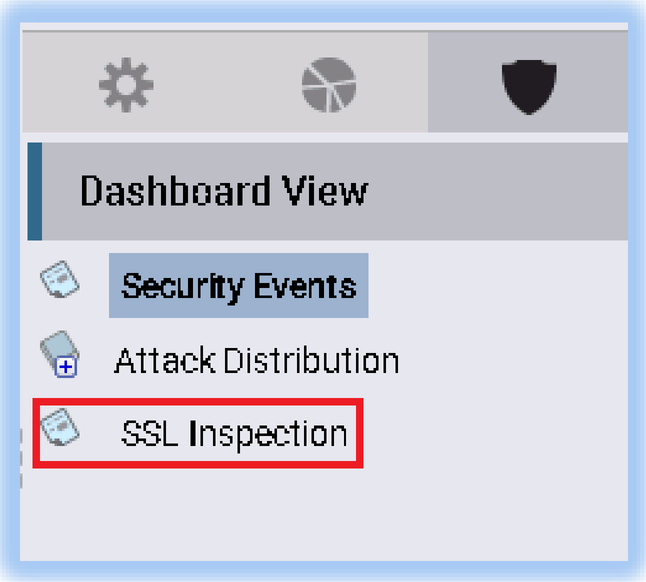
For any login issues, contact support@radware.com.

Welcome to Radware APSolute Vision!
APSolute Vision is the most comprehensive and effective solution for configuration, automation, monitoring, and reporting of Radware devices.



1. Click on the SSL Inspection Alteon and browse to the security monitoring tab:

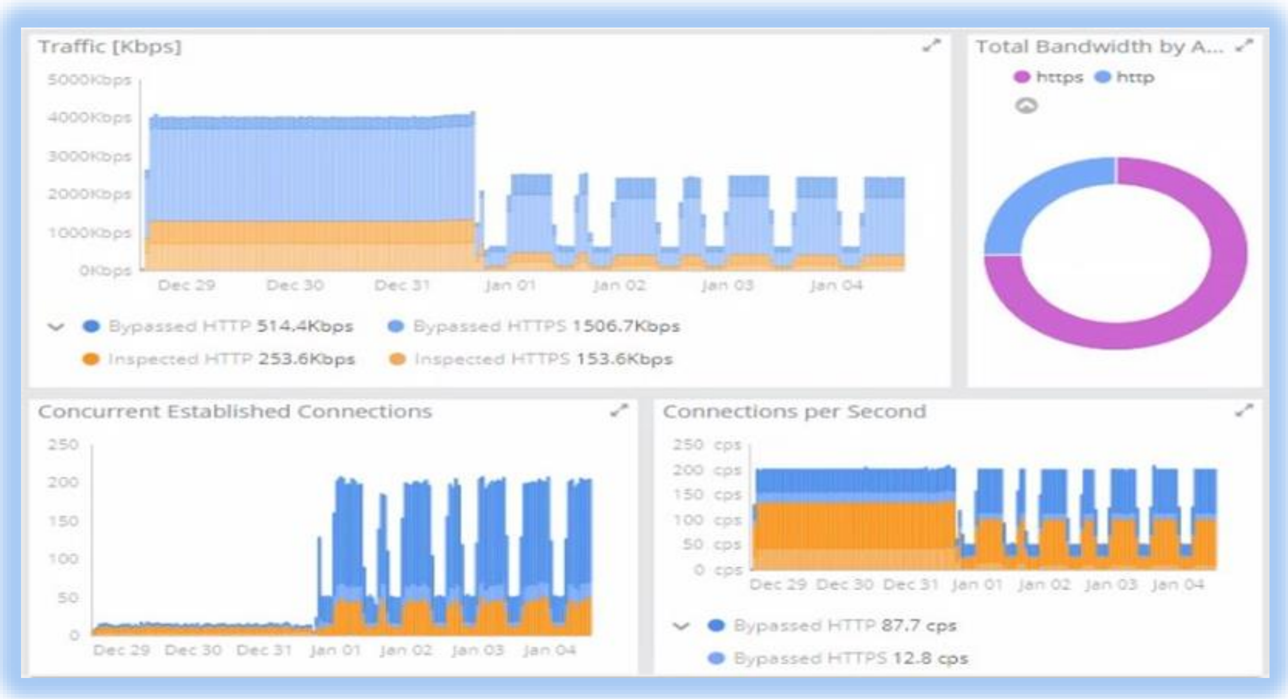
2. Click on SSL Inspection button:



The use of the demo lab and documentation is protected under the partner program guidelines and partner NDA and should not be shared with unauthorized parties.

All information provided in the Demo lab and documentation is provided “as is”. Radware makes no warranties, express, implied or otherwise, regarding its accuracy, completeness or performance

All SSL inspection analytics available on this screen:


Traffic [Kbps]
5000Kbps
4000Kbps
3000Kbps
2000Kbps
1000Kbps
0Kbps
Dec 29
Dec 30
Dec 31
Jan 01
Jan 02
Jan 03
Jan 04
Bypassed HTTP 514.4Kbps
Bypassed HTTPS 1506.7Kbps
Inspected HTTP 253.6Kbps
Inspected HTTPS 153.6Kbps
Total Bandwidth by A...
https
http
Concurrent Established Connections
250
200
150
100
50
0
Dec 29
Dec 30
Dec 31
Jan 01
Jan 02
Jan 03
Jan 04
Connections per Second
250 cps
200 cps
150 cps
100 cps
50 cps
0 cps
Dec 29
Dec 30
Dec 31
Jan 01
Jan 02
Jan 03
Jan 04
Bypassed HTTP 87.7 cps
Bypassed HTTPS 12.8 cps