Solution Brief

Seven Reasons to Deploy Blue Coat SSL Visibility with Application Delivery Controllers

Higher SSL visibility strengthens data center security.

Application Delivery Controllers (ADCs) are essentially advanced load balancers, using features such as compression, traffic shaping, SSL offload, and caching to optimize traffic flow among arrays of cloud content and application servers. Typically, they are not built specifically to increase visibility into SSL traffic. Today, with an increasing number of advanced threats hiding in SSL traffic, it is more important than ever to monitor and manage encrypted traffic in a data center – for security as well as production. The Blue Coat SSL Visibility Appliance, when used with ADCs, can fill the gaps in security coverage created by a lack of visibility into encrypted traffic. Here are seven specific ways the SSL Visibility Appliance can improve data center security when used with ADCs.

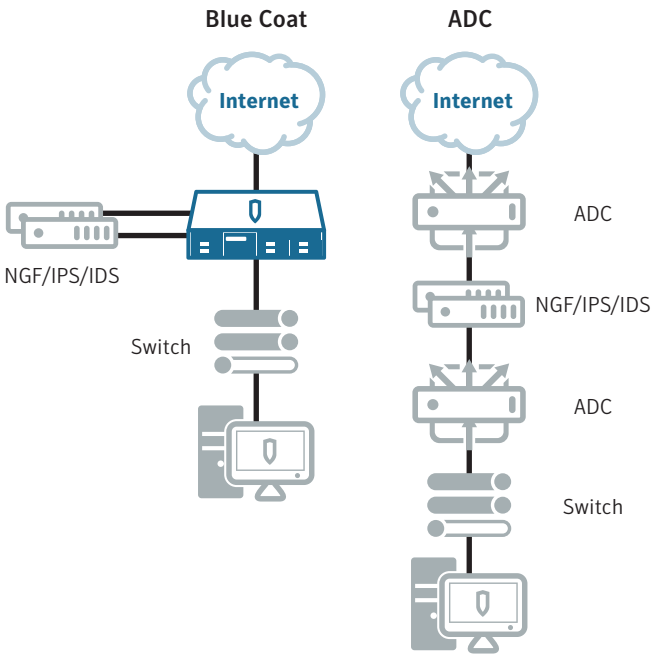
1 You can cut complexity while increasing SSL visibility

ADCs require a pair of boxes to decrypt and re-encrypt traffic. They are basically set up to decrypt traffic in only one direction for any virtual IP configuration instance. This coordinated two-box configuration is more complicated than a SSL Visibility Appliance configuration, and can require multiple switches or other devices for full traffic throughput redundancy. Scripting of the decryption devices may also be required when ADCs are used.

The SSL Visibility Appliance can decrypt traffic for analysis and filtering by multiple traffic analysis devices. In an in-line configuration, the SSL Visibility Appliance does this in both directions, so that encrypted traffic exiting the data center can also be screened for suspect traffic that in some cases is recorded in the SSL Visibility Appliance log.

In the Blue Coat configuration, each product does what it does best: the SSL Visibility Appliance provides visibility into encrypted traffic, and the ADCs manage servers. Some four-box high availability (HA) configurations do give ADCs the ability to load-balance security appliances, however.

Figure 1: Blue Coat SSL VA deployment vs. ADC deployment



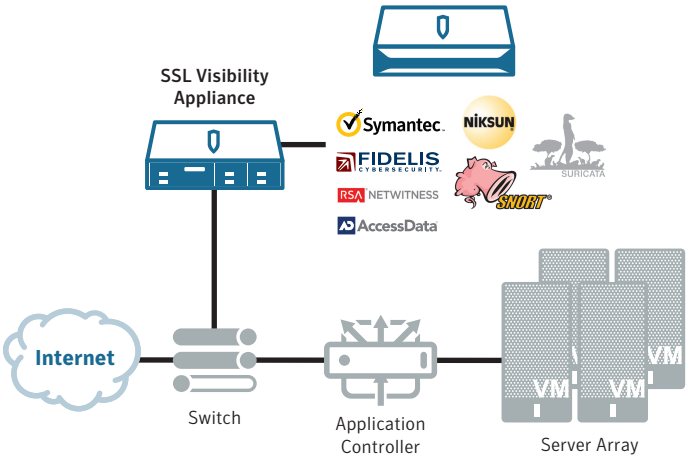
Symantec

2 You can increase SSL visibility without scripting or loading on the ADC

In many cases, data center traffic is decrypted and then re-encrypted so that network traffic is all encrypted. The ADCs can sometimes be programmed to mirror traffic directed to a VIP or client. However, this export loads the ADC and can require scripting on the device. In the case where inbound and outbound encrypted traffic is to be inspected, two scripts are often required.

The SSL Visibility Appliance can work off a single span port on a switch in passive mode to decrypt inbound traffic, so long as it has access to server keys and certificates using RSA SSL negotiation. This allows devices to see decrypted traffic and inspect it for attacks. Multiple devices of different types can be connected to the same SSL Visibility Appliance to receive the same decrypted traffic stream. ADCs generally have a single port for exporting decrypted data, and require additional equipment to feed multiple devices.

Figure 2: Simple SSL visibility deployment with Blue Coat



Note that if the SSL Visibility Appliance is placed in line, other SSL negotiation schemes can be used, and certificate resigning can replace server keys stored on the SSL Visibility Appliance.

3 You can avoid the risk of decrypted traffic being modified and forwarded in encrypted form

Many sites decrypt traffic on one device and then re-encrypt it on another. Not only is this traffic a security risk if it is found, but modifications to the traffic in decrypted form can be re-encrypted and forwarded as valid. In a situation where one box decrypts the traffic and another re-encrypts the traffic, there is no assurance that modification was not done.

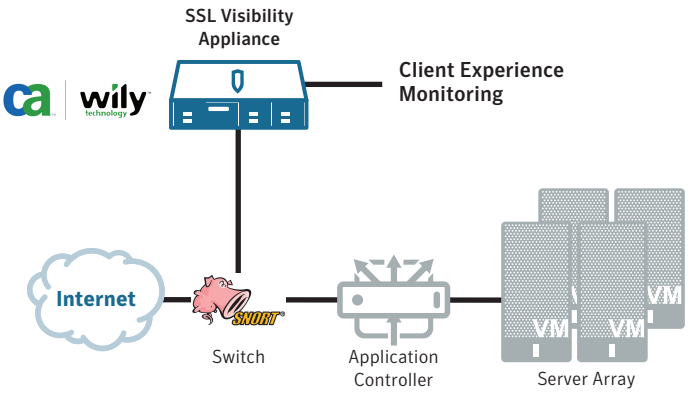
The SSL Visibility Appliance decrypts traffic, and only re-encrypts the original decrypted data sent to the security devices. This completely prevents compromise, re-encryption, and forwarding. This is the case even when the SSL Visibility Appliance is in active mode.

The SSL Visibility Appliance passes through the key negotiation between the client and server, and does not influence the choice of key exchange mechanism or cipher suite used for a connection. These are negotiated between the client and server and will be the same whether the SSL Visibility Appliance is present or not. Unsupported cipher suites can be either dropped or bypassed, but will be logged.

4 You can continue using application performance monitoring or user experience software

The performance of many large commercial applications such as Siebel, WebSphere, and BEA is often independent of the HTTP/HTTPS server states measured by ADCs. For this reason, application monitoring software such as CA Wily measures the user experience by identifying and timing transactions from individual users. This software needs decrypted traffic to do this, and the Blue Coat SSL VA provides a solution for this need.

Figure 3: Application Performance Management deployment



Performance monitoring software can operate in the “passive tap” configuration shown above where an RSA key negotiation is used.

5 You can detect more risks and threats through better logging

Unless they are scripted or in debug mode, Application Controllers do not do full logging of SSL status, but instead show management and HTTP/HTTPS actions. A typical log is shown below:

```
AX#show log
Log Buffer: 30000 Jan 17 11:32:02
Warning A10LB HTTP request has p-conn Jan 17 11:31:01
Notice The session [1] is closed Jan 17 11:31:00
Info Load libraries in 0.044 secs Jan 17 11:26:19
Warning A10LB HTTP request has p-conn Jan 17 11:26:19
Warning A10LB HTTP response not beginning of header: m
counterType="1" hourlyCount="2396" dailyCount="16295"
weeklyCount="16295" monthly Jan 17 11:16:18
Warning A10LB HTTP request has p-con
```

The Blue Coat SSL VA logs other parameters so that problems can be detected. These include:

- Clients forcing weaker encryption
- Certificate problems
- Specific protocol actions
- Unexpected SSL connections
- A sample of an SSL VA log is shown below

Figure 4: Sample Blue Coat SSL VA log

SSL Session Log 2/48

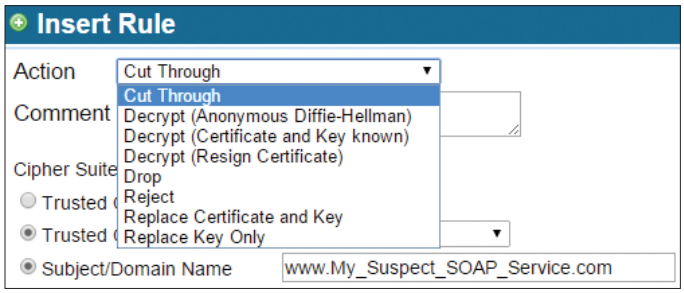
SrcIP:Port	DstIP:Port	Domain Name	Certificate Status	Cipher Suite	Action	Status
10.9.168.62:50110	65.55.138.112:443	fe2.update.microsoft.com	Valid	TLS_RSA_WITH_RC4_128_SHA	Decrypt (Resign Certificate)	Success
10.9.168.62:50109	65.55.138.112:443	fe2.update.microsoft.com	Valid	TLS_RSA_WITH_RC4_128_SHA	Decrypt (Resign Certificate)	Success
10.9.168.62:50108	65.55.138.112:443	fe2.update.microsoft.com	Valid	TLS_RSA_WITH_RC4_128_SHA	Decrypt (Resign Certificate)	Success
10.9.168.62:50107	65.55.138.112:443	fe2.update.microsoft.com	Valid	TLS_RSA_WITH_RC4_128_SHA	Decrypt (Resign Certificate)	Success
10.9.168.62:50102	157.56.141.102:443	watson.microsoft.com	Valid	TLS_RSA_WITH_AES_128_CBC_SHA	Decrypt (Resign Certificate)	Success

The graphic above shows that each SSL session is identified with its cipher suite and the processing associated with this connection. Exceptions such as invalid certs, bypassed SSL, and SSL failures all show up in this log to reveal site problems and vulnerabilities.

6 You can detect more risks and threats through better logging

The SSL Visibility Appliance can inspect traffic in both directions if it is installed in-line. This allows it to be used to identify outbound suspicious connections and limit them if it is in active mode. Blue Coat's categorization engine leads the industry in its ability to identify suspect and botnet control sites. Known domains, addresses, and certificate status problems can also be flagged and managed. The screen below shows the actions that can be taken on suspicious or other traffic.

Figure 5: Blue Coat SSL VA rule actions



A few of the categories that can be used to identify suspicious outbound connections include:

- Malicious Sources/Malnets
- Malicious Outbound Data/Botnets
- Scam/Questionable/Illegal
- Dynamic DNS (Addresses in the DNS scope of broadband providers, etc.)

Actions that are taken appear in the SSL log.

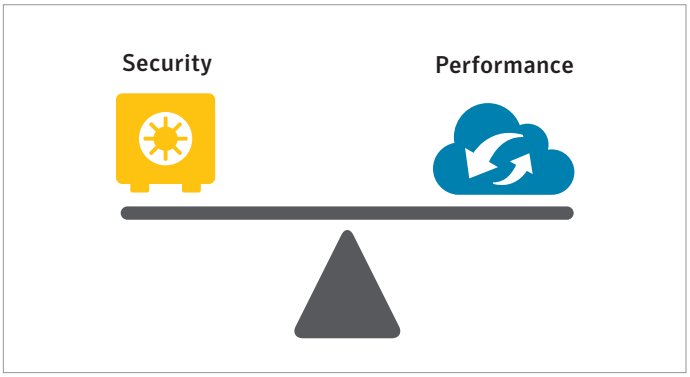
7 You have greater peace of mind knowing the solution is specifically built for security

Most ADCs are set up for high performance and known data center attacks. They are not designed as a general security device for detecting and securing all types of traffic. The SSL Visibility Appliance is designed by Blue Coat, a recognized leader in security technology, to decrypt and control all SSL encrypted traffic. To some extent, it can be a "second-opinion" on traffic going in and out of datacenters. It serves as a compliment to state-of-the-art Application Delivery Controllers by providing:

- Visibility and control of outbound encrypted traffic
- Use of other state-of-the-art security devices on encrypted data center traffic
- The world's best web traffic classification system (separate license)

The Blue Coat SSL Visibility Appliance provides an easy way of augmenting security to maintain a balance between security and the high performance requirements of a data center.

Figure 6: The security balance



Learn More

For additional information about Blue Coat solutions and technologies for SSL visibility and management, please visit Bluecoat.com/solutions/managing-ssl-and-https-traffic

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

Symantec Corporation World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

SYMC_sb_Top7_Reasons_Deploy_SSLVisibility_EN_v1c