White Paper

Criteria for Choosing the Right SSL VPN

Evaluating SSL VPN Solutions

AG Series Secure Access Gateways

Introduction

Remote connectivity is crucial for enterprise productivity, and SSL has become the *de facto* standard as a remote access tool. SSL VPNs as a technology offers much a deeper level of security than IPsec and other forms of remote access.

In today's crowded SSL VPN market, it's easy to become overwhelmed by the wide range of solutions available. Obviously, there are many factors to consider when purchasing an SSL VPN product, and you want to make the best choice possible. This SSL VPN evaluation guide serves as an important resource in identifying, describing, and prioritizing the criteria you should consider when selecting an SSL VPN solution that best fits the needs of your organization.

Selection Criteria

In coming up with a selection criteria, the functions offered by SSL VPNs have to be evaluated against two key aspects: security and user experience. A truly successful deployment of a secure access solution cannot be achieved without taking both aspects into consideration. Look for an SSL VPN that can also serve the organization's long-term needs, integrate seamlessly with the network architecture, and provide powerful management tools. The optimal provider will excel in these key areas:

- Performance and scalability
- Security
- Ease of use
- Company reputation
- Technology leadership

Security

In the case of SSL VPNs, the name itself implies one of the security measures being used. However, SSL does not make a VPN. In other words, encryption by itself is not enough to provide the security required for today's applications. The advantage offered by SSL VPN-based solutions lies in the combination of different layers of protection:

- SSL VPN Firewall
- Hardened OS
- Network Gapping
- Client Side Security
- AAA

- Reducing Network Exposure (Various Access Modes)
- Application-Level Filtering
- Virtualization and Network Separation

SSL VPN Firewall

Encryption can often be a double-edged sword; it is undiscriminating and offers confidentiality to both friend and foe. As a result of the encryption, any firewall positioned in front of an SSL VPN appliance cannot inspect the data sent to the appliance since it typically does not have the ability to decrypt the traffic. Without a firewall in front, an SSL VPN appliance is exposed to all sorts of network threats, and for this reason it needs firewall capabilities. These capabilities should include Denial of Service (DoS) protection (including DDoS protection) and apply the protection from the network through the application layers.

Key Questions You Should Ask Vendors:

1. Does the appliance have any type of firewall capabilities?
2. What layers are these capabilities applied to?
3. What type of DoS/DDoS protection is available?
4. What is the effect on performance when utilizing these features?

Hardened OS and SSL Stack

Most operating systems expose network-related vulnerabilities due to their generic nature. Commercial operating systems like Linux, Windows and others are designed to serve a multitude of purposes and often these purposes contradict, thus creating exposure to attacks. It is well known that the weakest spot provides the most vulnerability.

Taking into consideration that an SSL VPN appliance is most likely exposed directly to all sorts of network threats (as described in the previous section and in conjunction with any firewall capabilities offered by the appliance) it is crucial that the underlying operating system be designed to perform specific duties and thus not expose any unnecessary interface (which can potentially turn into a vulnerability).

In addition, many SSL VPN vendors have based their SSL stacks on OpenSSL, an open source implementation of the SSL/TLS protocols. Since its launch in 1998, OpenSSL has had dozens if not hundreds of vulnerability reports, ranging from Heartbleed to POODLE to Logjam and more.

Key Questions You Should Ask Vendors:

5. What type of an OS is the appliance based upon?
6. What was done to the OS to reduce its exposure to attacks?
7. What type of tests were performed to assure the strength of the OS?
8. Does your product rely upon OpenSSL for production traffic?

The Gap

Since it is acting as a gateway to the corporate network, it is important that an SSL VPN appliance create a gap between the non-secured and secured networks so that end users cannot establish direct connections to secured resources and applications.

Key Questions You Should Ask Vendors:

9. Does the appliance implement any type of "gap" technology?
10. Does this technology prevent end users from opening direct connections to resources?
11. What throughput limitations does this technology present?

Virtualization/Network Separation

It is important to leverage the existing infrastructure to support multiple user communities, both internal and external. These communities could include employees, partners, customers, demo sites, etc. Each of the communities should have the option of their own independent look and feel and customization, and should be manageable by independent administration groups. In addition, users who are part of a particular community should never be able to get into another community's infrastructure.

Key Questions You Should Ask Vendors:

12. Does the device support multiple communities of interest on the same appliance?
13. What features are customizable on a per-community basis?
14. What protection mechanisms are built in to avoid users of a given community from getting access to resources associated with another community?

Application-Level Filtering

To achieve the fine granularity of access control that is required of SSL VPN solutions, the appliance should be able to enforce access control policies based on protocol content.

Key Questions You Should Ask Vendors

15. Is application filtering provided on the appliance?
    a. What protocols can be inspected with application-level filtering?

Client-Side Security

An SSL VPN appliance can inadvertently introduce the risk of unsecured devices getting access to secured network locations, thus it is crucial that an SSL VPN appliance provide client-side security facilities. These facilities should allow administrators to evaluate the risk posed by a mobile or remote workstation or mobile device (host checking) based on different parameters (determined by the administrator) and associate the result of the evaluation to the forms of access allowed to users utilizing that device (and thus prohibit access if it is determined the risk level is too high).

Client-side security should also allow administrators to eliminate any "footprints" that might be left behind during the course of a user session. Access to SSL VPN appliances is often based on the user's Internet browser, and therefore local cache entries might be stored in the browser. Client-side security should allow administrators to eliminate these entries. If SSL VPN-enabled access is accomplished via a browser and a user account, it is quite likely that users will use different PCs or mobile devices and not all of them will be company issued. The main risk posed by these machines is that confidential corporate information might be left behind by the user. To eliminate this risk, a remote desktop access application can be used to ensure that data never leaves the network, and thus cannot be left behind on a user's device..

For major smart mobile device operating systems, an SSL VPN app can also be employed to eliminate the risk of browser-based access by smartphones and tablets.

Key Questions You Should Ask Vendors:

16. Does the appliance offer host checking facilities? If so, what type of information can be checked on the host machine (i.e. anti-virus software, registry values, etc.)?
17. What browsers are supported?
18. Are administrative privileges required?
19. What operating systems are supported?
20. Does the appliance offer cache cleaning facilities?
21. Does the appliance offer a secure remote desktop functionality?
22. What level of access control can be enforced based on the client profile?
23 Is an app available for smart mobile devices, and if so what types of protections does it offer?

Authentication

Authentication is the first step in establishing the identity of a user. The majority of the complexity related to authentication has to do with integration. Most organizations have existing standard authentication interfaces (such as RADIUS or LDAP) in place, and the appliance should be capable of integrating with these interfaces without any special configuration.

A challenge exists when a non-standard interface is used such as legacy systems, databases and others. For these cases it is important that the appliance provide a customization infrastructure that allows for a quick integration with these non-standard interfaces.

A special case of authentication has to do with SSL client-side certificates. Client-side certificates are an additional level of protection for the establishment of SSL connections, requiring each client to identify itself with its own unique certificate. For SSL VPN appliances this process takes place before the login page is ever presented to the user, since the login page is presented over an SSL connection. In many cases the client-side certificate is used as the only identifier for user sessions (for example USB-based client-side certificates). For complete protection it is necessary to be able to associate user sessions with the content of the certificate.

Key Questions You Should Ask Vendors:

24. What authentication methods are supported (and what configuration is required)?
    a) RADIUS
    b) LDAP
    c) Active Directory
    d) NDS
    e) SecurID
    f) Certificate Based
    g) Local
    h) Others
25. Do any of the standard methods require server-side configuration?
26. How are different dual-factor or multifactor authentication interfaces handled?
27. Can authentication be turned off?
28. Can multiple authentication interfaces be supported concurrently?

Authorization

Role-based authorization is an important part of almost any security policy and regulation. Administrators need to be able to limit access to information and applications based on the user role

(or associations) within the organization. These policies should be flexible enough to answer the most complex requirements; they should also be as dynamic as possible so that changes and updates can be applied easily and quickly.

The most important factor related to authorization policies is the granularity of authorization they provide. For example a Web-based authorization policy that allows filtering based upon URL is more granular than an IP-based policy that prevents access to port 80 of a specific server.

In addition authorization policies often introduce significant integration complexities. Where should the policies be stored? How should they be associated with users and groups? To avoid these complexities and allow for a smooth integration, the appliance should offer the greatest flexibility possible, allowing for policies to be stored locally as well as on an external server, and it should also allow administrators to correlate between external information (its source is usually the external authentication server) with locally stored policies. In order for an SSL VPN solution to delivery highly granular access control, it needs to be able to enforce access control policies.

Key Questions You Should Ask Vendors:

29. What types of policies are supported (i.e. Web based, shared directory, TCP, etc.)?
30. Are policies defined as PERMIT or DENY policies?
31. When designing policies is it possible to apply "White List" and "Black List" approaches?
32. Can policies be associated with users, groups or both?
33. How are policies stored and retrieved?
34. Can policies be stored on external servers?
35. Can policies be stored locally on the appliance?
36. Can policies be retrieved locally based on information from external servers?

Auditing

An extensive audit trail is a primary requirement of all security-related regulations and policies. The audit information should be generated in formats that allow easy analysis for both security and status monitoring reasons.

Key Questions You Should Ask Vendors:

37. How is the audit trail provided?
38. What formats of logging are supported?
39. What information is logged?
40. What tools can be used with the logs?

Access Modes (Network Exposure)

SSL VPN solutions' original "clientless" access methods allowed them to overtake IPsec technology for remote and mobile access. As SSL VPN technology evolved and matured, several client-based options were introduced as well, mostly dynamic clients that require no pre-installation. However one of the key advantages of SSL VPN solutions remains the variety of access modes.

These access modes allow administrators to extend their applications with the least amount of network-level exposure possible, which in turn significantly reduces the risk posed to the network. Most SSL VPN solutions offer variations of the following access modes:

- Native Web application and file sharing support, and support for HTML5 apps developed for mobile environments (least network exposure)
- Thin client support (low network exposure)
- Client/Server application support, also known as redirection (moderate network exposure)
- Network-level access (full network exposure)

Naturally it is best to prefer the least amount of network exposure possible and therefore take advantage of native Web applications and file sharing support, and/or secure HTML5 apps for mobile devices. However, the reality is that there are many legacy networking applications deployed that require tunneling (such as redirection or full network-level access). It is therefore important to be able to offer the end-user a combination of access modes that will reduce network exposure on one hand, and provide convenient and easy access on the other. For example, HTML5 requires only a browser to seamlessly launch any access method, without the need for ActiveX, Java, or any other complicated an difficult-to-use endpoint technology.

Another example of such a case is the combination of network-level access and native file sharing. Although it might be possible to offer Windows file sharing through various tunneling services, it exposes the network to a variety of threats related to the ports that have to be open in order to allow this type of functionality. Therefore an administrator might choose to block these ports using authorization policies. In this case users can utilize the native file sharing offered by the appliance. This is only possible if users can use multiple access modes at the same time.

Key Questions You Should Ask Vendors:

41. What type of access modes does the solution offer?
42. What types of applications are supported?
43. What is the underlying technology (i.e. Java, ActiveX, etc…)?
44. Can it offer access to resources based on IP address, DNS host names or both?
45. What types of thin clients are supported?
46. Can it publish applications through MS Terminal Services?
47. Can it publish applications through Citrix Metaframe?
48. What configuration is required for Citrix integration?
49. How is the client delivered to the end-user?
50. How are versions being updated?
51. Are full and split tunneling settings supported?
52. How are IP addresses being assigned?
54. What is the underlying technology (virtual adapter, PPTP, L2TP, redirection)?
54. Can this mode coexist with the other access modes (for example, is it possible to use this access mode and native Web application at the same time)?
55. What operating systems are supported by this mode?

User Experience

The end-user experience is determined by a variety of factors:

- **Performance** – How fast data is accessed and applications are executed.
- **User Interface Customization** – The ability to provide users with an interface that will be intuitive for their knowledge level and needs
- **Intuitive Use** – Using the various access modes should be easy and intuitive. No or only minimal installation should be required and user interaction should be kept to minimum
- **High Availability** – Minimal downtime is required in order to assure access

The importance of the user experience is obvious and is the main factor of productivity. However it is also crucial to remember that a good user experience also reduces the volume of support and help-desk calls.

Performance

To gauge the performance abilities of an SSL VPN product, various parameters should be taken into consideration:

- **Maximum number of concurrent user sessions** – The maximum number of users that can be logged in at the same time
- **Maximum number of concurrent SSL connections** – The maximum number of SSL connections that the device can sustain. Assuming that each user session requires at least one connection, this number should be equal to if not greater than the maximum number of concurrent user sessions
- **Maximum number of SSL operations** – It is common practice with SSL devices to state the number of SSL handshakes per second (or key exchanges), however this is a narrow definition since it covers only a portion of the SSL activity. Therefore the definition of this parameter should encompass both the initial SSL handshake and the bulk encryption that follows
- **Maximum bulk encryption throughput** – Most of the encryption performed by an SSL VPN device is bulk, which is the symmetric encryption portion of SSL

These parameters must complement each other. For example, just supporting the right number of concurrent user sessions is not enough; the number of concurrent user sessions must be complemented by the proper volume of SSL operations (i.e. high transaction rate per second, high throughput). The trade off is clear: fewer operations/sec per user means slower performance and a poor user experience. Mismatched performance and scalability will lead to the purchase of additional units even if the initial units support the right number of concurrent user sessions.

Under no-load conditions, all appliances introduce some latency. But, the true mettle of an appliance comes across when the device is loaded at the levels to which it is expected to operate. The better devices should be able to handle higher throughputs while still providing an acceptable user experience.

Key Questions You Should Ask Vendors:

56. Does the appliance use hardware acceleration for SSL encryption?
57. What is the maximum number of concurrent user sessions?
58. What is the maximum number of concurrent SSL connections?
59. What is the maximum number of SSL operations per time unit?
60. What is the bulk SSL throughput?
61. What kind of additional latency is introduced by the appliance under no-load conditions?
62. What kind of latency is observed under the targeted work load?

User Interface Customization

The user interface of an SSL VPN appliance is usually made of different Web pages: login, portal, logout and various error pages. Different users, partners, employees from different departments, and others have different applications and information available to them. Access to these applications and information depends on many parameters such as their role and needs. Different users require different user interfaces; the page designed for employee access might not be suitable for partner access.

For an access solution to be effective the user interface must be customizable in a way that allows each group (not to be confused with security-related groups) to have the design that best fits their needs. For example, partner access login might be performed from within an existing partner Web site, whereas employees would go to a special URL designed for employee use only.

Customizing the user interface goes beyond a special layout for each group of users. Each organization has its own procedures and business logic needs. The need to synchronize certain files after authentication and integration with proprietary authentication databases are just some examples of those needs. An access solution must have a way to integrate and interact with such customization.

Overall, the user interface is an important component in a good user experience; it is also crucial for user productivity. An access solution with a poor user interface, whether it's a design or lack of custom business logic integration, will reduce the productivity of its users.

Key Questions You Should Ask Vendors:

63. What components of the user interface are customizable?
    a. Login page?
    b. Portal page(s)?
    c. Logout page?
    d. Error pages?
64. Can the pages be customized per user or group profile?
65. To what level can each of these pages be customized?
    a. Customizable logo?
    b. Customizable messages as part of an existing template?
    c. Integrating with existing organizational portals?
66. Is it possible to create anonymous pages, on which there is no vendor signature?

Intuitive Use

As described earlier, one of the strengths of SSL VPN solutions is the variety of access modes they provide. However these different options might create confusion for end users. It is therefore crucial that these different modes be as intuitive as possible and require the least user interaction possible.

Key Questions You Should Ask Vendors:

67. Do any of the access modes require pre-installation?
68. Do any of the dynamic components require manual triggering by the user?
69. Is Single Sign-On (SSO) supported?

High Availability

High availability is a part of the end user experience that should be completely hidden. The best user experience is a consistent one, with no or minimal downtime. This goal should be achieved within the overall security considerations.

Key Questions You Should Ask Vendors:

70. Does the appliance support high-availability?
    a. How is high-availability implemented?
    b. Can multiple units be clustered together?
    c. If so, is there a limit to the maximum number of units that can be clustered together?
71. Does the high availability require any special hardware?
72. Does the high availability require any special connections?

Management and Administration

Supporting all the different user-experience and security-related settings mentioned in earlier sections may translate into an administrative nightmare. It is for that reason that any SSL VPN appliance should address the following issues:

- **Management Interfaces** – CLI, Web user interface, etc.
- **Components Deployment** – How are the different dynamic components (ActiveX, Java applets, etc...) deployed to the end user?
- **Administrative Privileges** – Do any of the dynamic components require administrative or other privileges?

- **Administration Delegation** – Can the administrative load be delegated between different administrators?

Management Interfaces

The administrator experience of an SSL VPN appliance is as important as the end-user experience. Offering a variety of management interfaces can ease the complexity of the administration tasks, since it allows the administrator a selection of interfaces to better fit individual tasks.

Key Questions You Should Ask Vendors:

73. What type of management interfaces are offered by the appliance?
    a. Does the device offer a CLI for management?
    b. Does the device offer a Web User Interface?
    c. Does the device offer SNMP support?
    d. Does the device offer any programmable management interface that can be used in conjunction with other Network Management tools?
    e. Any others?
74. Can all administrative tasks be performed from any of the interfaces?
75. If not, which of the tasks can be performed in which of the interfaces?

Components Deployed

Most SSL VPN solutions deploy various components, depending on the functionality being used. The deployment of these components, if not performed seamlessly, may create a significant load on support personnel, and ultimately hike the cost of supporting such a solution. The components discussed in this section vary from dynamic components required for different tunneling services (such as Java applets) to host checking and cache cleaning at the end-user device level.

An additional consideration regarding the different components is whether they require administration privileges. For example ActiveX components will not execute for restricted users, Java applets might be blocked from accessing the network and standalone executables could require administrative privileges to be installed. In some cases these components require privileges only once while being installed and in others they require these privileges every time they are used. In any case the need for administrative privileges creates a significant deployment complexity and should be avoided as much as possible.

Key Questions You Should Ask Vendors:

76. What are all the components that are being used by the appliance (ActiveX, Java applets and different types of executables)?
77. For each of the components described above, what administration privileges are required?

Delegation

For operational convenience and security reasons, it is commonly required that different administrators be assigned to manage different communities. The appliance should provide a method that will allow for delegation of administrative roles between different administrators. The delegation should also allow for administrator buffering, essentially having different administrators for the same unit without allowing them to intervene with each other's responsibilities.

Key Questions You Should Ask Vendors:

78. Does the appliance allow for the definition of multiple administrators?
79. Can different administrators be assigned with different administration roles?
80. Does the appliance provide any type of separation or buffering between different administrators?

Conclusion

Proper selection of an SSL VPN device involves an understanding of today's and future needs, as well as careful evaluation of the capabilities of the different devices under consideration.

Array Networks can assist you in learning more about existing SSL VPN solutions and keep you informed on future developments, so that you can make the most informed decision about your company's secure access requirements. Learn more on our AG Series product page, our secure remote access solution page, or download a free 30-day trial version of the vxAG virtual SSL VPN appliance today.

About Array Networks

Array Networks is a leader in application delivery networking with over 5000 worldwide customer deployments. Powered by award-winning SpeedCore® software, Array application delivery, WAN optimization and secure access solutions are recognized by leading enterprise, service provider and public sector organizations for unmatched performance and total value of ownership. Array is poised to capitalize on explosive growth in the areas of mobile and cloud computing, analysts and thought leaders including Deloitte, IDC and Frost & Sullivan have recognized Array Networks for its technical innovation, operational excellence and market opportunity.

Mar-2017 rev. a