NETWORKWORLD

This story appeared on Network World at
http://www.networkworld.com/reviews/2011/032111-cisco-mobile-security-test.html

Cisco sets the bar for mobile security

Combination of always-on client, VPN/firewall and Web security gateway provides secure access for mobile end users.

By Joel Snyder, Network World
March 21, 2011 12:07 AM ET

Cisco has been a leader in remote access VPNs since 1999, and its latest release, the AnyConnect Secure Mobility Solution, will make both end users and network managers very happy, despite a few rough parts.

The AnyConnect Secure Mobility Solution (part of Cisco's Borderless Networks initiative) consists of three seamlessly integrated products: the AnyConnect Secure Mobility Client 3.0, the ASA Adaptive Security Appliance (firewall/VPN) 8.4 and Cisco IronPort S-series Web security appliance 7.1.

SMBs might feel left out in the cold

Customers aren't required to buy all three products, but we found that you get better performance and better functionality if you do. In our testing, AnyConnect Secure Mobility Solution is all about managed end-point client software that's always active, protecting enterprise users and enforcing security policy no matter where they are, on a multitude of devices and platforms.

And enterprise network managers will be especially pleased with features such as optimal gateway selection (which automatically picks the best gateway for a user based on network characteristics), end-point posture assessment and better performance over more diverse types of networks.

It all starts with the VPN concentrator

The starting point for any remote access VPN discussion is Cisco's ASA 5500 series Adaptive Security Appliance, a combination VPN and firewall, with optional anti-malware and IPS capabilities.

Although older Cisco VPN clients can connect to non-VPN devices, such as PIX firewalls and IOS routers, connectivity with the new client is more limited. To get the benefit of the AnyConnect client's full feature set, you'll need an ASA appliance. IOS routers, including the 2851, 1951, 3800, and 3900, can also accept AnyConnect clients, but don't support the full feature set.

Your best bet, then, is to use an ASA appliance, which ranges from the ASA 5505 (10 to 25 users) up to the ASA 5585X (5,000 to 10,000 users).

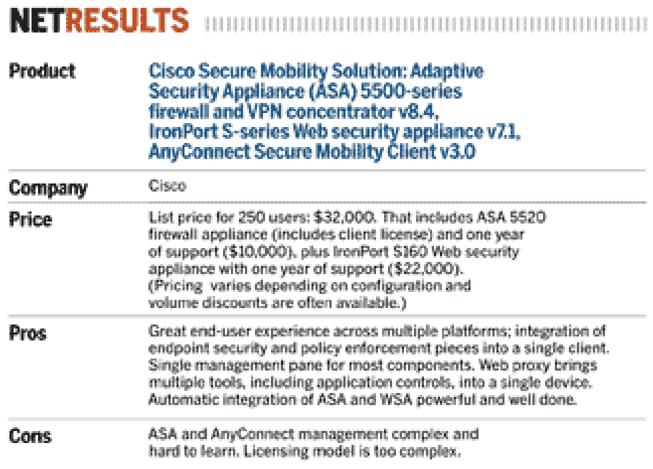
All ASA appliances have SSL VPN features, including reverse proxying (gatewaying Web applications at the application layer) and application tunneling (using encrypted tunnels to expose single applications through the VPN device), although we didn't focus on those features during this test. We spent most of our testing looking at network extension, bringing remote devices onto the corporate LAN, and Cisco's approach to securing those remote devices — what is now the traditional remote access use case. (Read Proxy configurations: The lesser of two evils.)

Next comes the client software

The next key component of a Cisco remote access solution is its new AnyConnect Secure Mobility client. The AnyConnect client has the basic feature set that one would expect in a mature product: end-point security detection and control, simplified deployment and policy downloading directly from the VPN gateway, wide-ranging user authentication options, and remote user policy enforcement features.

Cisco offers the AnyConnect client as an installed package available for all Windows versions back to XP, Mac OS X 10.5 and 10.6, Intel-based Linux distributions with the 2.6 kernel, Apple iOS 4 (the iPhone and iPad operating system), and Windows Mobile versions 5 and 6.

The AnyConnect VPN client is not required to make a VPN connection to an ASA appliance — you can still use the built-in VPN clients in Windows and Mac OS X, Nokia's Symbian phones, iPhones, iPads and iPods, as well as Cisco's older multiplatform Cisco VPN client, and a host of third-party clients.



NETRESULTS

Product	Cisco Secure Mobility Solution: Adaptive Security Appliance (ASA) 5500-series firewall and VPN concentrator v8.4, IronPort S-series Web security appliance v7.1, AnyConnect Secure Mobility Client v3.0
Company	Cisco
Price	List price for 250 users: $32,000. That includes ASA 5520 firewall appliance (includes client license) and one year of support ($10,000), plus IronPort S160 Web security appliance with one year of support ($22,000). (Pricing varies depending on configuration and volume discounts are often available.)
Pros	Great end-user experience across multiple platforms; integration of endpoint security and policy enforcement pieces into a single client. Single management pane for most components. Web proxy brings multiple tools, including application controls, into a single device. Automatic integration of ASA and WSA powerful and well done.
Cons	ASA and AnyConnect management complex and hard to learn. Licensing model is too complex.

Click to see: Net results

However, you give up a lot of performance, functionality and features if you don't use it. For example, the AnyConnect client can use IPSec, SSL/TLS, or DTLS (SSL/TLS run over UDP instead of the normal TCP). We found that shifting from SSL/TLS (TCP) to DTLS (UDP) with the AnyConnect client gave us between 40% and 45% increase in total performance, depending on the characteristics of the Internet connection. DTLS and traditional IPSec had similar performance characteristics. In our testing, traditional IPSec edged out DTLS by a few percentage points in most tests, but the performance difference was difficult to perceive.

Another key feature of the AnyConnect client not found in Cisco's older IPSec clients is end-point security checking, remediation, and control. Taking a cue from the SSL VPN and NAC worlds, Cisco has folded its Cisco Secure Desktop into the AnyConnect client (for a price — there is a license fee), and has merged desktop security management into the VPN concentrator, tremendously simplifying the task of linking desktop and VPN security policies and avoiding the potential for things to drop between the cracks.

Web security is the final piece

The last major piece of Cisco's remote access solution is a new addition: the Cisco IronPort S-series Web Security Appliance. The IronPort S-series is a secure Web gateway, with the primary goals of protecting Web-browsing end-users from malware and enforcing access controls on where people can browse.

We didn't do a full evaluation of the product, focusing only on its integration with the ASA and VPN clients. But the IronPort S-series has the expected feature set for a Web security gateway: malware scanning using multiple engines, URL filtering to avoid bad neighborhoods and enforce acceptable use policies, bandwidth management, and the ability to look at content to enforce general security policies, such as blocking PowerPoint attachments.

The IronPort S-Series includes "man-in-the-middle" SSL decryption, which lets it scan both encrypted and un-encrypted connections, and leverages the IronPort reputation service to do reputation-based lookup of URLs and Web servers. This feature set makes it a fairly complete Web security gateway, not all that different from the other market-leading products.

We focused on integrating the IronPort S-series with the ASA appliance, and applying Web security gateway policies to remote access VPN users. A cynic might say that Cisco requires network managers to buy a whole separate box — and an expensive one at that — because they don't have built-in Web security in the firewall. That's true, of course, but it's also true that the Web security in the IronPort S-series is more powerful than what you can get with the Web security feature built-in to unified threat management firewalls.

Kicking it Old School

Even if you're satisfied with your current VPN deployment and are on an upgrade cycle, with no plans to turn on any new features, you'll be happy with the new products because they make life a little easier.

Forced upgrades rankle Cisco customers

For example, if you already know how to run Cisco's older VPN 3000 GUI, you'll see that most of the VPN parts have been transplanted into ASDM, Cisco's Java-based ASA appliance management tool Adaptive Security Device Manager.

The ASA appliance can be your source for the VPN client software, and you don't have to build pesky policies that get glued into the AnyConnect client at installation time, so you can have a VPN deployment up and running more quickly than using the old client and old hardware.

The AnyConnect client is also more firewall-friendly, falling back to SSL/TLS encryption over the Secure-HTTP (443) port, which means less frustration for end users on the road. And ASDM includes a VPN wizard, to guide you step-by-step and help automatically glue together the bits and pieces that all have to match to make things work.

Legacy licensing

Well, there's actually one problem that will frustrate VPN 3000 users: licensing. The ASA appliance is really the next generation of PIX firewall, with a merging of the best VPN features from both the PIX and the old VPN 3000. One of the features carried over from the PIX is feature-based licensing, and the ASA licensing can best be described as "you've got to be kidding."

For remote access feature set alone, there are 6 types of licenses, with another half-dozen types for the platform itself. For inexplicable reasons, you need a special license to also use mobile devices with your ASA appliance, although only if you use AnyConnect client software, and not if they use the old client, and don't forget the special license for your IronPort S-series WSA to make it part of the Secure Mobility Solution.

Fortunately, there's a 48-page manual which explains it all — make sure you sit down and read it through a few times before you start. Our only other advice is to be sure to get your strong encryption license (it's free, fast, and online; you just have to promise not to let your ASA slip into the wrong hands) before you start, because encryption profiles will only be correctly set up using the wizards if the strong encryption license is already installed.

Putting the pieces together

Cisco Secure Mobility Solution is not just a VPN toolkit; it's about enforcing enterprise security policy when staff members are both in and out of the office. That means you'll need to spend some time thinking about your security policy before you begin configuration.

One of the important things to remember about the AnyConnect client is that it is "always on," meaning that it enforces security policies based on the location of the user, even when there is no tunnel in place. The AnyConnect client periodically connects to the ASA even when the client is not running — you'll see these little 20 packet exchanges to the HTTPS port of the ASA as it verifies that the ASA is alive and well and doesn't have a new policy to hand out.

You can change the security policy on the fly, so you don't have to get it perfect before you start your deployment, but it's a good idea to know where you want to end up before you start. Because the configuration tools within ASDM are so complicated, the only way to avoid getting lost is to zero in on what you want to accomplish. Building policy is only easy to do if you know what you want to enforce.

Cisco could have done a much better job in ASDM of making things consistent and usable. In the VPN part of the GUI alone, there are dozens of options and a confusing and contradictory set of terms. This makes it easy to make mistakes, or build a less-secure deployment because you didn't get everything done correctly.

For example, split tunneling can be done with a much higher level of granularity than was available previously, a great security improvement. But digging out the different features and getting them properly configured involves multiple screens and "Advanced" tabs that have to be opened. The result is that it's easier to not use this new feature, and have a less secure deployment.

While much of the VPN feature set can be configured using the command-line interface (CLI), making full use of the feature set requires you to use ASDM. The basic encryption and tunneling tools are all CLI-based and CLI-debuggable, but some parts of the client-side policy configuration rely on hidden files on the internal flash that are best left to ASDM to keep straight.

We built a basic ASA firewall using the CLI, and then we stuck entirely with ASDM. Once we got all of the licensing pieces worked out, our final configuration with RADIUS authentication, end-point security checking, and Web-based downloading of the AnyConnect client from the ASA appliance only took about an hour.

But that configuration was done with the help of one of Cisco's trainers. The solution has a lot of moving parts, and without hands-on guidance, we could have spent days covering the same territory. If you can possibly afford the time, sit down and read through the documentation or take some training.

Happy end users

The good news is that while the Secure Mobility Solution can be complex for network managers, it's a fantastic experience for end users. Think of yourself as throwing yourself on your sword to help everyone who's actually going to use the remote access VPN. No matter what platform we tested — Mac, Windows, and iPhone were in our lab — getting the client installed and operational was simple. If end users liked the old Cisco VPN client, they'll love AnyConnect, which has a modern feel and brings benefits beyond just VPN tunnels.

For example, on the Windows platform, AnyConnect client includes Network Access Manager (NAM), which is a full-fledged 802.1X supplicant for wired and wireless networks. Since AnyConnect client is meant to be used both on the corporate network and while roaming, integration of 802.1X features lets a single client package handle end-point security and connectivity.

AnyConnect is your network-access control (NAC) client (with 802.1X and end-point security checking, remediation, and enforcement) when in the office, and your VPN client (with IPSec and SSL transports, as well as the same end-point security features) when on the road. Even better, the AnyConnect client can figure out where you are by using a feature called Trusted Network Detection, which looks at domain names and DNS servers being handed out via DHCP. This can help automate the process of choosing whether to use 802.1X and NAC or bring up a VPN tunnel. In our testing using an Enterasys C2 Ethernet switch, Trusted Network Detection and the 802.1X supplicant both worked without any hitches.

It's hard to describe how complete the AnyConnect client experience is without turning this test into a laundry list of features. Cisco has done a good job of covering all the bases, supporting both strict and loose security policies, as well as multiple deployment options (such as pre-installing the client or letting end-users download it from the ASA appliance using a Web browser) and authentication settings (such as whether the VPN client launches before the user logs into Windows or after). We tried a good assortment of these features and found that in this area the AnyConnect client worked as advertised.

We had mixed success with end-point security posture checking. Basic host scanning is included as part of the ASA AnyConnect Premium license, while remediation features (such as forcing an anti-malware update or turning on a desktop firewall) require the Advanced Endpoint Assessment license.

Part of the difficulty in end-point security within the AnyConnect client is that the policy is spread across different parts of ASDM. For example, you look for the presence of a particular anti-virus package in one part of ASDM, but you look to make sure you're not executing in a virtual machine in a completely different part of the policy.

The ASDM management tool lets you build a posture checking decision tree using traditional flow-chart symbols, a technique that looks suspiciously like the one F5 pioneered in their SSL VPN product. In any case, this configuration approach to end-point posture checking is approximately 10,000% more understandable and scalable than Cisco's old approach based on the ACS RADIUS/TACACS server.

The AnyConnect client's end-point security approach represents Cisco's current thinking on how to do both NAC and VPN posture checking in the same client. Cisco is continuing to avoid the Trusted Computing Group's open standards for posture checking, and has forged ahead with a single-vendor solution, incorporating its own Cisco Secure Desktop and OPSWAT's end-point posture checking toolkit together into a single nicely merged solution. (The Oesis Framework, an OPSWAT product, is a software library incorporated in other security products that detects the presence and state of a wide variety of end-point security products.)

Overall, network managers will have to balance the simplicity of Cisco's strategy, which requires only a single client and no particular cooperation from the end-point security vendor, with a lock-in to what Cisco and OPSWAT are willing to support.

Our experience with OPSWAT, which has shown up in both our NAC and SSL VPN security tests for years, has generally been good, although we have had recurrent difficulties getting consistent results when testing against our lab's standard anti-virus package, Sophos. This experience was echoed in this test, where different configurations of the same anti-virus package gave different results in the AnyConnect client. Network managers using the AnyConnect client to do end-point posture checking will want to experiment with their own configuration and end-points to avoid false positive and negative results.

Web security goes to the cloud

Cisco's Secure Mobility Solution has three specific strategies for protecting end users from the vast wasteland of the Internet: end-point security, cloud-based security, and enterprise proxy protections.

On the end-point, the AnyConnect client with its Cisco Secure Desktop feature set doesn't provide much protection itself (beyond a basic personal firewall), but can be used to detect the state of end-point security and, with the purchase of an Advanced Endpoint Assessment license, perform some limited controls.

The second strategy, cloud-based security is offered in conjunction with ScanSafe, a recent Cisco acquisition. Cisco has incorporated the ScanSafe client tool into the AnyConnect client and the ScanSafe policy management tool into ASDM, making the option of deploying cloud-based malware scanning and Web filtering functionality fairly simple. ScanSafe licensing is completely separate from all other Secure Mobility licensing, and ScanSafe is only supported on Windows platforms.

While the integration makes it easy for an enterprise to select cloud-based scanning, we think that most enterprises will see cloud-based scanning vs. enterprise proxy protections as an "either/or" choice. From a policy point of view, Cisco has put a very light touch on the whole ScanSafe interface.

For example, while the AnyConnect Client has a trusted network detection feature, ScanSafe also has a similar feature. Rather than combine the two, each runs independently, letting ScanSafe work in a non-AnyConnect environment. Similarly, all of the Web-based security policies established on the IronPort S-Series Web proxy are completely independent of the policies set up for ScanSafe; you can't reuse any of the components and you can't easily translate the policy from one to the other.

We chose to focus on the third type of Web security: the Web proxy. Cisco's approach to applying Web-based security to VPN users requires a tight linkage between the ASA VPN concentrator and the S-series Web proxy, in order to transfer authentication information to the Web proxy. Making that linkage is very simple — you just put a common port number and shared secret into both devices, click the "test" button, and if everything is correct, you're done.

The ASA sends the username, but not any group membership information, over to the IronPort S-series, so we had to link to our Active Directory (NTLM or LDAP are supported) to get this information. Once that was settled, we were able to apply user- and group-based Web security policies.

One of the most important parts of the integration between the AnyConnect client, the ASA appliance, and the IronPort S-Series is the automatic download of proxy information to AnyConnect clients. We tested this with Windows (Internet Explorer), Mac (Safari, Chrome, and Firefox), and iPhone systems all running the AnyConnect client and had seamless experiences browsing through the VPN tunnel, passed to the IronPort S-Series proxy, and off to the Internet.

The IronPort S-series has a fairly standard set of protections, including URL filtering (for example, blocking gambling sites), malware scanning with two different engines (Webroot and McAfee in our test system), and Web reputation checking, used to block access to known bad Web pages or objects. The IronPort S-series also supports sanctioned man-in-the-middle, a way to "break in" to the SSL conversation by pretending to be the encrypted Web server with a fake public-key infrastructure certificate.

We briefly tested the malware scanning and URL filtering. As with all URL filtering products, we had a very high success rate, but were able to slip through a few URLs in violation of policy. A selection of 10 recent viruses transmitted into our test lab network were all caught by the malware scanner.

We 'like' the Facebook controls

A new feature in the IronPort S-Series is application visibility and control. This lets the network manager monitor and block various Web-based applications directly, separately from the URL filtering part of the product. The version we tested is more of a proof-of-concept than a fully-baked application visibility tool, with only eight categories, including "Blogging," "Facebook," "IM," "LinkedIn," "Media," "P2P/File Sharing," "Conferencing," and "Social Networking."

These are a bit of a mish-mash of different applications, many of which could be caught by simple URL filtering. However, the idea behind application visibility appears to go beyond the simple block/allow/warn of URL filtering, and get more specific in the controls.

For example, Facebook is broken down into 15 subcategories, such as "Facebook Applications: Games" and "Facebook Applications: Education," which would allow you to differentiate different types of Facebook usage, blocking those you don't allow. In our testing, the S-Series was able to differentiate different types of Facebook usage and blocked access accordingly. In fact, Facebook is one of the most sophisticated sets of controls. For example, you can block all Facebook Events, or you could just block posting of events but allow "Like" of events. In LinkedIn's controls, you can block the employment section separately from the messaging section, or you can block job searches separately from job postings.

In our testing, the IronPort S-Series did exactly what it said it would — identify applications and apply application controls, including bandwidth limits, as a Web proxy. However, it's clear that for this to work, you need a proper configuration.

For example, now that many Facebook users are selecting to encrypt their sessions, you must use the sanctioned man-in-the-middle to decrypt the SSL, or there's no possibility of applying fine-grained application controls. Similarly, if you want to control BitTorrent, you must force the traffic through the proxy by blocking VPN users who try and go around the proxy.

Overall, the Web security options within Cisco's Secure Mobility Solution give network managers enough choices to provide strong policy enforcement for end users no matter where they are.

Snyder is a senior partner at Opus One in Tucson, Ariz. He can be reached at Joel.Snyder@opus1.com.

Read more about security in Network World's Security section.