NETWORKWORLD Reprint

THE CONNECTED ENTERPRISE = APRIL 10, 2017

INSIDER CLEAR CHOICE TESTS

Fight firewall sprawl

The Algosec security policy management toolset delivers orchestration and automation.

BY JOHN BREEDEN II, NETWORK WORLD

New and innovative security tools seem to be emerging all the time, but the frontline defense for just about every network in operation today remains the trusty firewall. They aren't perfect, but if configured correctly and working as intended, firewalls can do a solid job of blocking threats from entering a network, while restricting unauthorized traffic from leaving.

The problem network administrators face is that as their networks grow, so do the number of firewalls. Large enterprises can find themselves with hundreds or thousands, a mix of old, new and next-gen models, probably from multiple vendors -- sometimes accidentally working against each other. For admins trying to configure firewall rules, the task can quickly become unmanageable.

That is where Security Policy Management comes into play. These products used to be called firewall managers, and in truth, they mostly still just manage firewalls - though some also help with routers and switches. They allow administrators to define security policies, and then rely on the programs to - somewhat automatically – make it happen.

We looked at security policy management programs from AlgoSec, Tufin and Skybox. Each suite was deployed and tested in a virtual and physical environment stacked with firewalls from all the top vendors including Palo Alto, Cisco, WatchGuard, Check Point and others. We deployed new security policies, tracked and identified traffic flow complications, decommissioned old or non-functional rules and checked configurations against desired security policies and regulatory requirements.

> "We were most impressed with AlgoSec."

While each suite did an excellent job, we were most impressed with AlgoSec, although not every organization might agree with us. What set AlgoSec apart was that it allowed end users, not just security teams, to help share the burden and take ownership of managing security policies as they related to their areas of responsibly within an organization.

The Tufin suite seemed targeted at top-level security professionals, but nonetheless had an intuitive graphical interface which made diagnosing traffic and security policy problems extremely easy. Tufin was also the only suite which had full end-to-end functionality with the AWS cloud, including complete automation.

Skybox had the most comprehensive security suite of any that we tested, with a ton of extras available in the form of other modules to help in areas like vulnerability management and threat intelligence. It was also the most economical when only deploying the firewall management module.

NET RESULTS

COMPANY	**AlgoSec**
PRODUCT	Security Policy Management Suite
PRICE	Starts at $30,000
PROS	Innovative, solid features and functionality, gives end users some responsibility for managing their own security policies
CONS	Gives end users some responsibility for managing their own security policies

AlgoSec Security Policy Management Suite

The AlgoSec Security Policy Management Suite aims to automate the process of securing even the most complex firewall deployments, letting valid traffic pass through network gateways unharmed, while stopping all threats. The level of automation is customizable based on an organization's comfort level.

> "Of all the products we tested, AlgoSec was the most innovative."

It can provide simple help with rule creation at the low-end to true zero touch deployments where applications and processes can be authorized without human intervention. With granular controls, users can even start small with something like automatic processes requiring human approval, and then automate their security policies slowly over time as they become more comfortable with the concept of taking their hands off the wheel and letting their systems manage themselves.

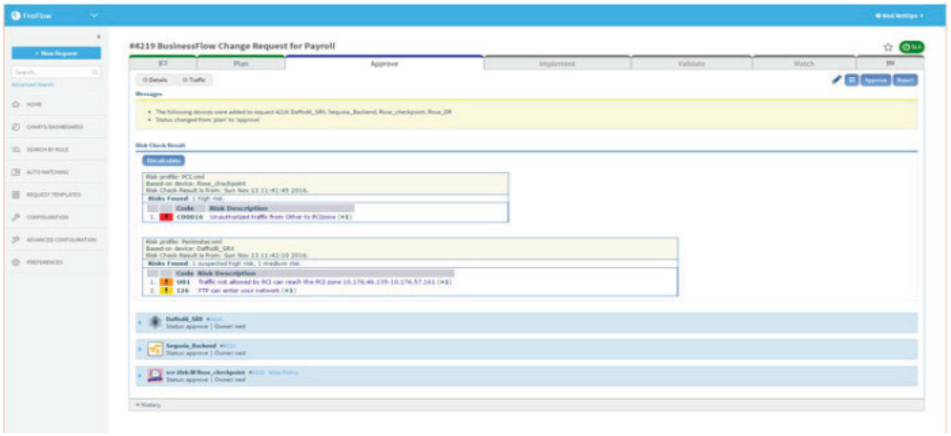
Of all the products we tested, AlgoSec was also the most innovative in that it put a lot of effort into empowering application owners. Most products had a little bit of that, but only AlgoSec created an interface with good permission-based roles tailored to help non-security personnel assist in crafting security policies that affect their work. This may require a change of thinking or culture at some organizations, but AlgoSec put tools in place to ensure a successful deployment.

The AlgoSec Security Policy Management Suite has four components: AutoDiscovery, BusinessFlow, FireFlow and Firewall Analyzer. They are tightly integrated to the point that it's easy to drift from one component to another, though some like AutoDiscovery, which finds the connectivity links between devices, is likely going to get used most often. The software starts at $30,000 and can vary based on network size.

Once in place, the interface for AlgoSec will change depending on who is looking at it. The program offers single sign-on, with each user thereafter being shown a dashboard populated only with data they are

responsible for, and what they are authorized to see. This might lengthen onboarding times because more users beyond just the security team can be given access, and each user's role needs to be defined.

We configured several application owner type users who were not part of the security team and had them working along with security personnel. Much of the setup was done using out-of-the-box templates, but specific network and user information still needed to be configured.



> "AlgoSec can handle the whole process automatically."

Once set up, application owners who logged into the system were shown the health of the apps each was responsible for maintaining. In one example, a certain app was not achieving full functionality in our dashboard. We could highlight the application and get information, in mostly plain English, about the problem.

For application owners, AlgoSec tries to simplify things as much as possible. Instead of being shown information about IP numbers or firewall configurations, we were simply told that, in this example, our app could not connect to either a Washington D.C. or a California-based time clock server, which was hurting functionality. That's all we needed to know at that level.

From the user level, we highlighted the problem and created a ticket which then went up the chain to security personnel. The highlighted problem came up on our dashboard when we re-logged in as an administrator. From that view, the entire AlgoSec suite opened up for us. We could run a traffic simulation with BusinessFlow through a virtual network and see why the time servers were getting blocked, in addition to finding the IP numbers and devices in that chain. It turns out that a Check Point firewall was blocking the traffic.

As an admin, we could dive into the specific rules and the reasoning behind the blocked traffic. In this case, there was a low probability that allowing FTP traffic to return from the clock servers could open an FTP hole in the network. There is almost no chance that a time clock server is going to get compromised and used to inject FTP attacks, but the danger was there, so Check Point was stopping return traffic, hurting the needed app. Knowing this, we chose to allow it, which automatically rewrote the rules on the blocking firewall. We could have also sent the matter up to higher authorities for approval.

Depending on the level of automation set, AlgoSec could have also automatically approved the change the user wanted. We reset the network and reprogrammed the suite to allow all changes of minimal risk or those with no risk at all. After that, when the user made the same request, it was quickly approved and acted upon. An audit trail was still generated, and AlgoSec ran a post-rule change diagnostic to ensure that the change did not negatively affect anything else, but security teams were never bothered with the fairly trivial event, other than being sent a notice about it. The user was able to instigate the change even though they really didn't know anything about firewall management, or even what device was ultimately blocking their app.

> "The AlgoSec Security Policy Management Suite is extremely innovative."

Another innovative thing about AlgoSec is that all rules can be future-proofed against obsolescence, and the suite won't propagate new rules which overlap existing ones. It's interesting to be thinking about decommissioning devices and rules while they are being first deployed and programmed, but that is what AlgoSec does, or can be set to do if desired. Going back to the FTP time clock server rule as an example, when approved, or at any time afterwards, we could set an expiration date. For our tests, we set it to just a few minutes, but normally the expiration date would be months or even years in the future.

When the expiration date arrives, the application owner who requested the rule is queried, asking if they still need the rule or rule change in place. If they do, then the rule can be recertified. But if the server or application no longer exists or has been migrated elsewhere, like into the cloud, then the owner can simply tell AlgoSec that the rule is no longer needed. At that point, security teams are notified and can decommission it to avoid unnecessary clutter, or to stop the organization from taking on any risk that is no longer necessary. And if set to do so, AlgoSec can handle the whole process automatically.

The same care goes into the process of deploying rules. When we made a new rule to block specific HTTP traffic between the cloud and physical parts of our test network, we were told that some of our firewalls were already effectively doing that because of other rules. As such, we only needed to deploy the new rule to certain devices. AlgoSec remembers all those relationships and rationales too, so that if the would-be duplicate rules are ever decommissioned or changed, it doesn't open a hole in the defenses.

The AlgoSec Security Policy Management Suite is extremely innovative, allowing users to help shoulder the burden of security, automating the process of creating new firewall rules, reducing rule-based clutter and helping to safely deploy and decommission devices as needed. And if an organization isn't comfortable with any of that, it can be ignored and used like any other firewall manager program, though that would be a shame given the functionality and time-saving features packed into this advanced toolset.

John Breeden is an award-winning reviewer and public speaker with over 20 years of experience. He is currently the CEO of the Tech Writers Bureau, a group of influential journalists and writers who work in government and other circles. He can be reached at jbreeden@techwritersbureau.com.