sageza

Instant Insight
February 13, 2006

Cisco Applies Unified Field Theory to Security Management

By Joyce Tompsett Becknell

Cisco has announced the new Cisco Security Management Suite, an integrated set of security management applications that provide an operational framework for system-wide security policy enforcement and administration. The suite is made up of the Cisco Security Manager (CSM) and a new version of the Cisco Security Monitoring, Analysis, and Response System (CS-MARS) version 4.2. The suite has integrated monitoring, configuration, and management, for identifying and enforcing data monitoring policies. Cisco believes that these applications will simplify support for Cisco's Self-Defending Network security strategy which is focused on identifying, preventing, and adapting to an ever changing security and threat landscape.

The CSM includes:

- Different views at the device, policy, and topology levels. While the device and policy levels focus on their respective components, the topology view offers a virtual representation of the network that scales through linked network maps and includes firewalls, Virtual Private Networks (VPNs), and Intrusion Prevention Services (IPS).
- Capabilities that allow policy abstraction and sharing: separation of the policy from devices enforcing it so it can be shared and applied to other devices.
- Ability to provide distributed deployment of policies with workflow capabilities for change management and compliance processes.

The new version of CS-MARS includes:

- Improved dynamic and real-time event viewing and categorization capabilities and expanded device support.
- Along with CSM, the ability for administrators to quickly identify exactly which device and policy is responsible for allowing or denying traffic.

Cisco also announced a new Content Security and Control security services module (CSC-SSM) for the Adaptive Security Appliance (ASA) 5500 Series which provides "Anti-X" services, and which was developed in alliance with Trend Micro. The Anti-X services provide unified antivirus, anti-spyware, file blocking, anti-spam, anti-phishing, URL blocking and filtering, and content filtering.

Net/Net

The trend of 2006—if it can be posited in February—is management. It is impossible to speak to a vendor or IT manager and not fall into a discussion of the importance not only of management, but of how to do it well. Just as the IT world built islands of automation, of applications, and of compute power, so too it has built islands of management. There is network management, systems management, storage management, change management, services management, and so forth. It wouldn't be going too far out on a limb to suggest we

The Sageza Group, Inc.
32108 Alvarado Blvd #354
Union City, CA 94587
510·675·0700 fax 650·649·2302
London +44 (0) 20·7900·2819
Milan +39 02·9544·1646

need some management of all that management. Security hasn't really been thought of as a management issue, it's been thought of a security issue although that's changing—Cisco envisions security as a fundamental part of the network—and many of its large enterprise customers would agree with them. In that light, Cisco's approach to security has continued to evolve in lockstep with its vision of the network. This announcement is some of the first we're seeing from Cisco's more integrated approach to security, and it's spot on.

While most organizations now realize that true security requires a holistic mindset that approaches systems rather than components, it has been easier to envision than to realize. First off, it has been difficult to find solutions on the market that function holistically. Until now, Cisco's offerings fell into this trap as well. In general, customers could create policies for the organization, but then each device or class of device was monitored in its own way. Additionally, there was no topological view for understanding the interrelationships between devices on the network, so that when something happened, it required time to sort out and respond completely. Making sure a similar attack couldn't happen again was also difficult to do without a topology view to easily sort out similar configurations within the network. The organic evolution of security within the network commenced by embedding security features where appropriate into devices, or setting up systems to monitor, track, and respond to specific types of threats. The maturing market is now leading to integration of these capabilities across the network.

The ability to view policies and devices separately means that policies can be made at the corporate level and then repetitively implemented on devices wherever it is sensible to do so. A graphical overview of topology helps customers be able to spot exactly where threats are occurring as well as to know additional similar vulnerabilities that can all be addressed together. Cisco has had some success with the CS-MARS product. While customers will be able to purchase either product separately if they so desire, we suspect most of them will want to take advantage of the more integrated suite. Cisco customers who run large networks and worry about integrated security should be thinking about a product like this as their next step. As Cisco grows its customer base, we assume they will build a database of best practices and use that to help customers more quickly implement their product.

There is certainly a lot of work to do in the management space, and most of the major vendors have focused at least part of their R&D or M&A efforts to that end. Looking forward we find ourselves thinking about the next challenges. Since most IT organizations already use at least one dashboard, there are long-term questions about what and how IT will manage. We suspect that like most markets, eventually there will be three dominant players and several smaller, more niche-like players, and at this point, they could be any of a handful of vendors. Regardless of who ultimately emerges and their philosophy of management, we suspect that interoperability and integration will be key issues. To that end we can only encourage vendors like Cisco to continue to ensure that they are thinking of all forms of security and management, and not just those implemented at the network layer. The other direction this takes of course is federation, or integration between organizations. Once internal security is coordinated, IT organizations will be required to synch their security with those of their partners, suppliers, and customers. This will be even more complicated than internal security, but just as important in the long run. Without products like CSM in place, it will be impossible.

The Sageza Group, Inc.
32108 Alvarado Blvd #354
Union City, CA 96587
510·675·0700 fax 650·649·2302
London +44 (0) 20·7900·2819
Milan +39 02·9544·1646