Webtorials

Q&A WITH . . . CISCO

Borderless Services Node (BSN) Delivers Integrated Wired, Wireless Policies

Cisco is bundling several modular components into a package for the company's Catalyst 6500 switching platform that together comprise the Cisco Catalyst 6500 Borderless Services Node (BSN). The BSN package includes a Catalyst Virtual Switching Supervisor Engine 720; a Wireless Services Module (WiSM), which is a Cisco WLAN Controller module for the Cat 6500; and two Firewall Services Modules (FWSMs).

Independent editor/analyst and Webtorials contributor Joanie Wexler sat down with Shweta Goyal, product manager in Cisco's Cloud Switching and Services Technology Group, to find out more about the ins and outs of the new solution.

What's the thinking behind packaging a WiSM and two firewall modules together for use in the same switch chassis?

GOYAL: Traditionally, enterprises have viewed "infrastructure" and "services" as two separate functions. If the service is security, then a separate security team typically manages it. This introduces complexity, because the network infrastructure cannot be detached from security enforcement gates. With the BSN, Cisco is offering a way to combine the security and wireless decision-making points, rather than keeping them separate as they have been in the past.

How specifically will the bundle benefit enterprise customers?

GOYAL: Typically, enterprises have had to create separate policies for wired and wireless campus users. Now, you can enter policies into the FWSMs and let them be shared by wired and wireless users. This constitutes a huge operational savings for network administrators; it keeps security policies consistent, which makes the overall network more secure.

Can you actually create and enforce policies across both networks from a common management system?

GOYAL: Polices can be created and enforced through the same firewall management system using either Cisco Security Manager (CSM) or Adaptive Security Device Manager (ASDM).

Does that mean I no longer need a Cisco Wireless LAN Controller (WLC) or Cisco Wireless Control System (WCS) to manage my wireless LAN?

GOYAL: No, you will need WLC and possibly WCS to manage your wireless LAN. But rules can be configured for any IP address on the network and enforced from the firewall management platform; it doesn't matter if the IP address belongs to a wired or a wireless device. We are also making enhancements to CiscoWorks LAN Management Solution (LMS), our switch management software, so that we can provide an interface to manage both the FWSM and WiSM from one entry point.

Why do you call the package a "Borderless" Services Node?

GOYAL: With the ability to provision, secure and manage users across both their wired Ethernets and their wireless LANs, enterprises can connect users located anywhere at any time using any device, and they can do so securely and reliably. These are the characteristics of a "borderless organization" and hence the name "Borderless Services Node."

What role does "virtual switching" play?

GOYAL: The Cisco Virtual Switching Supervisor 720-10G contains network virtualization technology that allows any two Cisco Catalyst 6500 Series Switches to be pooled together into what we call a Virtual Switching System (VSS) 1440. The VSS 1440 acts as a single virtual Catalyst 6500 switch, enabling the two switches to share a single point of management, a single gateway IP address and a single routing instance. It also eliminates the dependence on First Hop Redundancy Protocol (FHRP) and scales system bandwidth capacity to 1.4Tbps by activating all available bandwidth across redundant Catalyst 6500 switches.

What is the importance of eliminating the dependence on FHRP?

GOYAL: Typically, in a standalone environment, FHRP is required to provide a single default gateway that is both redundant and highly available. In a Cisco VSS environment, FHRP for redundancy is no longer necessary, because a single interface and router MAC address are shared across both virtual switches. Replacing FHRP (a software-based failover mechanism) with multi-chassis EtherChannel (a hardware-based failover mechanism) improves network availability for delay-sensitive applications such as video and voice. Removing FHRP also makes network management simpler, as you no longer need to concern yourself with VLANs being active/standby on the different switches.

Is there a reduction in pricing when buying the WiSM and two FWSMs components in the newly created package?

GOYAL: Yes, users receive approximately one third off what the components would cost when purchased separately.

Are there different versions of the BSN?

GOYAL: Yes. The BSN can come equipped with a 24-port, 1Gbps Small Form-factor Pluggable (SFP) fiber module or with a 16-port, 10Gbps Ethernet fiber module. Which configuration you choose depends on the speed at which you want to connect your

access network layer to your distribution switch (the BSN). The BSN with the 1Gbps configuration has a 35% discount, while the BSN with the 10Gbps ports has a 33% discount, compared to buying the components separately.

Why are two firewall modules useful or needed?

GOYAL: One WiSM today can support 300 APs with a throughput of 8Gbps. One Cisco Firewall Services Module has a throughput of 5Gbps, so we are packaging two firewall modules together with the WiSM to ensure that security performance keeps pace with the WiSM backplane performance.

What level of virtualization is there in the BSN?

GOYAL: The BSN can be partitioned into 250 virtual firewalls per FWSM. This means you only have to buy one physical firewall instead of several. BSN can also enable network virtualization on both Multiprotocol Label Switching (MPLS) and non-MPLS networks. This can be used to segment different groups within an organization. With the help of virtual firewalls, the same segmentation can be extended from the campus to the data center. In fact, one of our existing customers has scaled up to 400+ virtual routing instances to enable virtualization in the campus using the same components available in the BSN. For a more detailed discussion on network virtualization, visit the following http://www.cisco.com/en/US/solutions/collateral/ns340/ns517/ns431/ns658/net_qanda0900aecd804a16ae.html

Why would an organization need 250 firewalls?

GOYAL: In a campus environment such as a university, there might otherwise have to be a physical firewall in each building. This might be the case, for example, if the departments want to restrict access to their data from other users and departments or to enable granular control. An organization may want to separate all their multicast traffic, services, wireless users, point-of-sale systems and guests and put them on their own virtual networks, for example. This would be expensive to buy and operate if using separate physical firewalls. Creating virtual firewalls means it no longer matters where the physical firewall is sitting, so doing so breaks down physical location capex and opex barriers.

Could you explain campus network virtualization?

GOYAL: Network services virtualization within the campus helps IT focus on providing a unique set of policies to different network segments without having to deploy dedicated service nodes. Some organizations may segment their network based on division boundaries; others may do so for compliance reasons to segregate confidential traffic from general user traffic.

How does this approach affect an enterprise's IT processes?

GOYAL: Different teams typically manage the IT department and security department. However, it doesn't have to be this way. We have discovered a large number of enterprise customers that need to divide their network into multiple virtual campuses. Each virtual entity would like to manage their infrastructure and security

on their own to exercise finer controls and custom policies. BSN provides the IT owners a mechanism to manage resources centrally but allow departmental control within the virtual network.

Is Cisco asking IT departments to overhaul the way they manage and secure their local networks to use the BSN?

GOYAL: The change is being led by evolving enterprise needs. Organizations are finding themselves in the middle of a transition where the network border is disappearing, and the way networks are built, managed and secured must evolve in step. Cisco is helping with that by making it more affordable and deployable.

Will the BSN enhance the actual interoperability of the firewall and WiSM modules or are they functional islands within the Cat 6500 that just happen to be located in the same chassis?

GOYAL: Interoperability per se is not enhanced, but the FWSM and WiSM are not islands anymore, either, because enterprises gain new ways to segment their wireless users. They like the ability to provision the same policies for both wired and wireless users from one interface. They also like that the services are integrated in the same chassis as their network device. It simplifies their physical rack and network design. They are also looking for Cisco to provide best practice recommendations for deploying these different technologies together. BSN provides enterprises that synergy.

How so?

GOYAL: Wireless VLANs map to virtual “security contexts” – available hardware resources partitioned among different virtual firewalls. The virtual security contexts, in turn, map to a virtual routing instance. This setup makes sure policies remain intact across networks. For example, if a user needs to switch from one VLAN to another, the virtual security context will inspect the policy to make sure none of the policy conditions are being violated.

Can the BSN play a role in helping organizations comply with various auditing and security mandates, such as HIPAA, SOX and PCI?

GOYAL: Yes, that was one of the drivers behind creating the BSN. Unified policies based on identity of users sharing the same WLAN and LAN infrastructures can be enforced for end-to-end compliance. For example, one of the requirements for Payment Card Industry (PCI) compliance is that the enterprise needs to segregate the network that carries credit card transactions from user traffic. BSN enables that.

Can you provide a brief roadmap of your plans for the BSN?

GOYAL: In the future, we will have higher performing service modules and a supervisor that will scale the system beyond current capacity along with other software enhancements. We are also working with lead Cisco solution architects on ways to simplify the deployment of the solution so that it is easy for our customers to adopt and deploy. ❑

Interviewer Joanie Wexler *has spent 20 years writing about IT and computer networking technologies, their business potential, and implementation considerations. Among her areas of specialty are mobile/wireless communications and emerging wide-area networks.*

About the Webtorials® Editorial/Analyst Division

The Webtorials® Editorial/Analyst Division, a joint venture of industry veterans Steven Taylor and Jim Metzler, is devoted to performing in-depth analysis and research in focused areas such as Metro Ethernet and MPLS, as well as in areas that cross the traditional functional boundaries of IT, such as Unified Communications and Application Delivery. The Editorial/Analyst Division's focus is on providing actionable insight through custom research with a forward looking viewpoint. Through reports that examine industry dynamics from both a demand and a supply perspective, the firm educates the marketplace both on emerging trends and the role that IT products, services and processes play in responding to those trends.

For more information and for additional Webtorials® Editorial/Analyst Division products, please contact Jim Metzler at jim@webtorials.com or Steven Taylor at taylor@webtorials.com.

Published by Webtorials Editorial/Analyst Division
www.Webtorials.com

Division Cofounders:
Jim Metzler
jim@webtorials.com
Steven Taylor *taylor@webtorials.com*