

[fw-wiz] Nokia 5300 or Cisco Firewall Services Module

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2003-11/0022.html>

From: Camilo Tesone (*camilo.tesone_at_verizon.net*)

Date: 11/06/03

To: <firewall-wizards@honor.icsalabs.com>

Date: Thu, 6 Nov 2003 15:50:34 -0500

Hi,

I was wondering if anyone had experience with Cisco's Firewall Service Module. We're trying to decide between two Nokia Checkpoint boxes (Nokia 5300s) and two Cisco PIX FWSMs. Any feedback would be appreciated.

The architecture is a server farm in which over 200 servers attach to two Cisco Catalyst 6513 switches.

The two Catalysts are connected to each other via EtherChannel trunks and are serving the same VLANs. Each Catalyst 6513 has a MSFC (router) for outside connectivity and redundancy (via HSRP). The design provides for redundancy for the servers should one Catalyst fail.

Our goal is to protect one or more VLANs with firewalls. Integrating firewall protection into this architecture involves purchasing two firewalls. One firewall would attach to one switch and the other firewall would attach to the other switch.

Each protected VLAN/subnet would be served by both firewalls. Since both switches serve the same VLANs, this simply means putting one interface on each firewall on the same VLAN on their respective switches. If one firewall goes down, the hosts on that protected VLAN continue to use the other firewall on that VLAN. Each firewall will have one interface assigned to an "outside" VLAN, which connects to the outside world via the routers in the two Catalyst switches. We are running HSRP for each routed segment.

The Cisco FWSM will provide for stateful failover, but will not load share. The Nokia's can be set up in a cluster and will provide for stateful failover and also load sharing. This is more attractive, but there are other requirements.

1. Scalability. The Nokia's support up to a max of 8 Gigabit Ethernet interfaces while the FWSM can support up to 100 protected interfaces.
2. Throughput. The Nokia 5300 has a max throughput of 5 gigs while the FWSMs

Firewall-Wizards: [fw-wiz] Nokia 5300 or Cisco Firewall Services Module

can handle up to 10 gigs.

3. Cost. Each FWSM would cost us about \$20K after a sizeable discount. I think the Nokias are a little cheaper but I don't know yet. We will not have to pay annual maintenance on the FWSMs from Cisco because maintenance is already included for each module in a Catalyst 6513 once you purchase support for that chassis. The Nokia maintenance would be expensive.

4. Ease of use. This includes the ability to create and modify rules, groups etc.

Thanks again for anyone willing to provide their insights.

firewall-wizards mailing list

firewall-wizards@honor.icsalabs.com

<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>