Addition Questions and Answers for RFP #648689

1. Is VA Tech looking for an “IDS Like” syst “IPS Like” system? Does VA Tech want to have a system that can actually mitigate traffic or detect only? If it is detect only, how does VA Tech plan to actually mitigate a Rate Based Attack or large scale Malicious Traffic Based attack? How will VA Tech plan to mitigate an attack? Actively Mitigate or passively Detect then take evasive action? If it is the latter, how quickly does VA Tech plan to react to any attack?

We are seeking a product that can mitigate as well as detect traffic.

2. From the diagram the device would not be an inline device but would hang off of the ISB Border Switch/Router. Is this the only configuration that is acceptable to VA Tech?

The diagram is only for informational purposes. The product can be placed inline off the ISB border or border/switch routers.

3. From the diagram, what type of ports off of the ISB Border Switch/Router can be provided? Would they be Bi-Directional SPAN Ports?

The unit may or may not be connected to bi-directional SPAN ports depending on other constraints. Caveats for uni-directional SPAN port operation should be included. The border router is Catalyst 6500 series switch with a SUP720 module.

4. Is Distributed Denial of Service (DDOS) a concern for VA Tech? What is the plan to mitigate a large DDOS attack with an “IDS Like” device?

DDOS attacks are a concern to VA Tech. The product should be able to mitigate DDOS (Botnet) attacks.

5. What is the IPv6 requirement where the “IDS Like” device is connected off of the ISB Border Switch/Router? Will IPv6 traffic be encapsulated in Piv4 at this point?

“IPv6 currently traverses the ISB Border Router”.

6. What is the future physical connectivity requirement where the “IDS Like” device is connected to the ISB Border Switch/Router. Is it GigE long term or is it 10GigE? What is the actual traffic loads at this point? What is the plan to move to 10Gig?

Current connectivity requirements are single gigE. Peak Traffic loads are 700Mbit/sec, sustained load is ~450Mbit/sec. There are plans to move to 10Gig within 24 months, the traffic may exceed 1Gb peak load within 12 months and VA Tech would like link aggregation support information.
7. Is the requirement strictly defined by the diagram to connect devices between the two ISB Border Routers and the ISB Border Switch/Router? Is asymmetrical traffic a concern? Also what are the future connection speeds between the ISB Border Routers and the ISB Border Switch/Router?

The diagram is strictly for information purposes only. Future connection speeds between the ISB border routers and ISB border switch router will be 10GigE.

8. Is VA Tech looking to provide all of the requirements with a single device or is multiple devices a possibility?

A multiple device configuration is acceptable.

9. There are devices that have the ability to provide “IDS Like” functionality in two fashions. First if set up using SPAN ports, the device must still see all traffic bidirectionally. Second the device can be set inline but be placed in “Hardware Bypass Mode” where all traffic is detected but none is mitigated. Which method does VA Tech prefer?

The table shown on P.6, 2 a) asks how the products handles those states. There is no preference implied.
Additional Questions and Answer for RFP 648689

1. Are there any firewalls between: a) Remote Access & ISB Core Switch/Router b) ISB Border Router & ISB Border Switch/Router?

There are no firewalls installed at the border.

2. Is the requirement for inspection of IPv6 for “Native” IPv6 traffic?

Yes, native IPv6 traffic passes through the border router.