

United States

Department of Veterans Affairs



VA Approach to Meeting the OMB IPv6 Mandate

April 2007

Prepared by:
IPv6 Working Groups

1 OBJECTIVE

The Department of Veterans Affairs (VA) is committed to the successful deployment of Internet Protocol version 6 (IPv6) across the VA IT infrastructure. Over the next 12 to 15 months, the primary effort will be to focus on the requirements and deadlines of the IPv6 mandate identified by OMB. The requirements for June 2008, as set forth by OMB, include the following:

- a. **INBOUND**
Transmit IPv6 traffic from the internet and external peers through the network backbone to the LAN.
- b. **OUTBOUND**
Transmit IPv6 traffic from the LAN through the network backbone out to the internet and external peers.
- c. **INTERNAL**
Transmit IPv6 traffic from the LAN through the network backbone to another LAN or another node on the same LAN.

2 SUMMARY

The VA intends to accomplish the IPv6 transition and meet the OMB requirements by March 2008, mitigating risk to the VA IT enterprise by using a controlled approach, defining a subset of VA-managed IPv6-enabled backbone devices, and taking advantage of business case opportunities.

3 APPROACH

The following approach will be taken to achieve success in meeting the requirements of the OMB IPv6 mandates for capabilities to be met by June 2008. This approach does not address the longer term testing and deployment of IPv6 across the VA IT enterprise beyond June 2008.

VA intends to test IPv6-enabled components from a representative sample of each of the various affected equipment configurations that exist across the VA IT enterprise. The remaining VA network hardware and software will be made "IPv6 ready" only to the extent of ensuring that all other applicable equipment is capable of being set up and configured to the tested profiles (e.g. with sufficient memory, correct IOS, etc.). In other words, the implementation will be based on requirements for IPv6 rather than installing and activating IPv6 on all 1500+ routers across the entire enterprise, precluding current testing and/or pilot(s) with IPv6.

- a. The scope of initial IPv6 testing will be defined by establishing categories of devices that are involved in the One-VA WAN backbone and Internet gateway infrastructure (such as LAN/WAN routers, switches, firewalls, IPS, etc.).

- b. Within each category, the number of different equipment configurations that exist across the One-VA WAN backbone and Internet gateway infrastructure (by manufacturer, model, IOS, etc.) will be identified.
- c. Mirror configurations for each category will be established in the IPv6 lab environment and tested to ensure that each configuration in each category is capable and compatible, from an IPv6 perspective. The setup/configuration for each configuration and category will be documented for use as a template at other sites for testing and future deployment purposes.
- d. Selected sites that are representative of each of the configurations and categories will be identified and tested according to the OMB criteria (see *Section 1 - Objective*). This testing will be done across the One-VA WAN backbone and Internet gateway infrastructure when the appropriate security analyses has been completed and the requisite security components have been put into place.
- e. Upon successful completion of the OMB test set at all of the test locations, it will be concluded that all other instances of the same tested configurations and categories of devices located elsewhere within the One-VA WAN backbone and Internet gateway infrastructure will pass similar tests.
- f. When the OMB-mandated testing is complete, IPv6 capabilities introduced into the VA enterprise will remain enabled on the One-VA WAN backbone and Internet gateway infrastructure to facilitate continued technology and business case assessments. Continuation or removal of IPv6 capabilities will be contingent on a complete assessment of potential risks and measures available to mitigate those risks.
- g. Testing results will be documented (see *Section 4 - IPv6 Test Case Templates* for examples) and provided to the VA CIO and OMB along with rationale and test procedures.

Note: No application enablement is planned for inclusion in these tests.

4 IPv6 TEST CASE TEMPLATES

4.1 Test Case 1 – Inbound

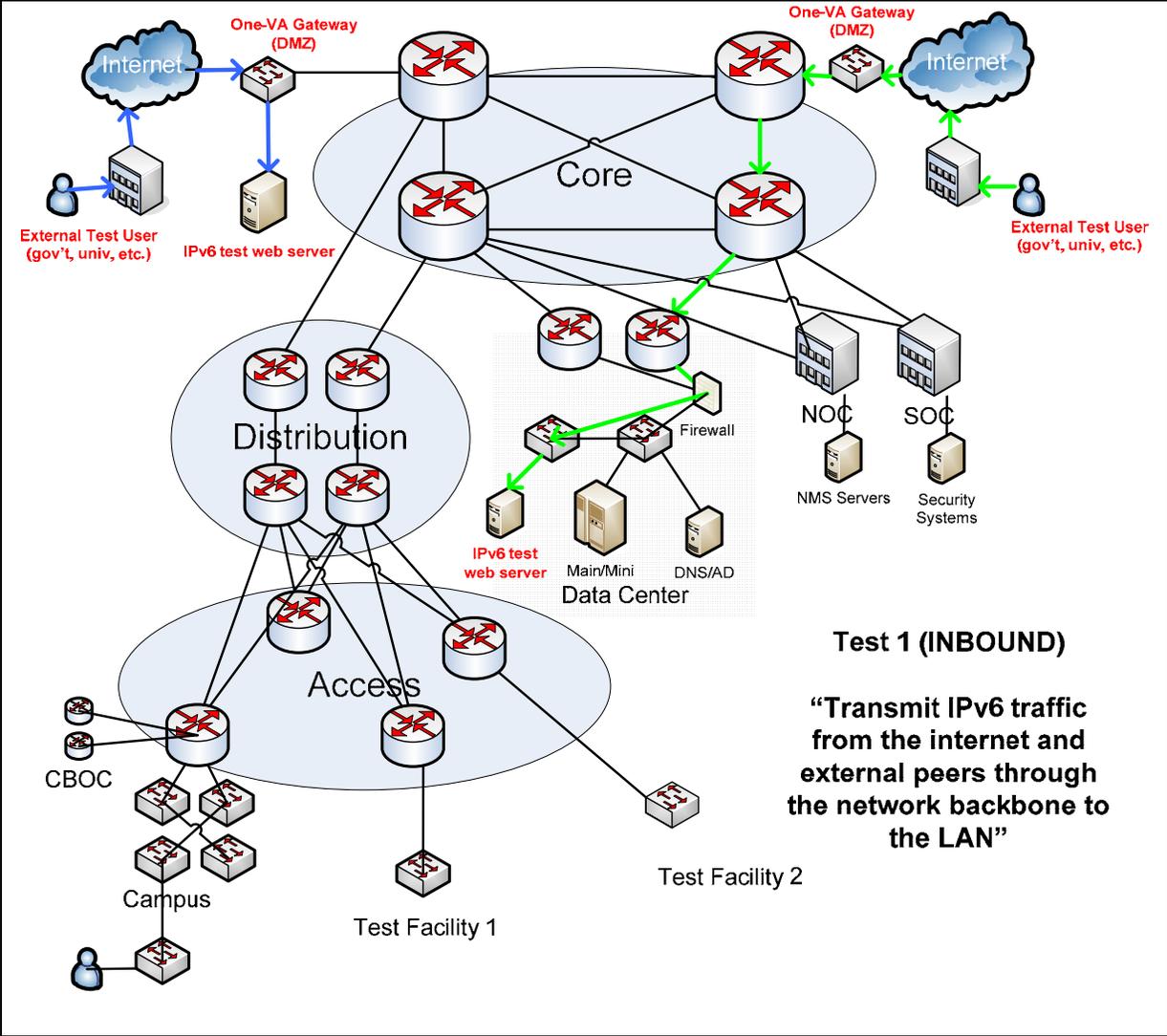
INBOUND <i>“Transmit IPv6 traffic from the internet and external peers through the network backbone to the LAN”</i>	External Location #1 Name: sixxs IPv6 Tunnel (www.sixxs.net) Traffic Direction: Source Site Type: IPv6 External Client	External Location #2 Name: Internet2 IPv6 Partner Traffic Direction: Source Site Type: IPv6 External Business Partner
VA Site #1 Name: Reston ECSIP DMZ Traffic Direction: Destination Site Type: Typical Internet DMZ	Test: #1, #2 Test Results:	Test: #1, #2 Test Results:
VA Site #2 Name: Falling Waters Data Center Traffic Direction: Destination Site Type: Typical VA Web Server Hosting Facility	Test: #1, #2 Test Results:	Test: #1, #2 Test Results:
VA Site #3 Name: TBD Traffic Direction: Destination Site Type: TBD	Test: #1, #2 Test Results:	Test: #1, #2 Test Results:

Proposed Tests

1. Set up and access a Web page inside the VA using an IPv6 address as the destination and an IPv4 address on the Web server.
2. Set up and access a Web page inside the VA using an IPv6 address as the destination on a Web server running a native IPv6 stack.

Success Criteria

1. The Web page hosted on an IPv4 Server is accessible via an IPv6 address.
2. The Web page hosted on an IPv6 Server is accessible via that IPv6 address.



4.2 Test Case 2 - Outbound

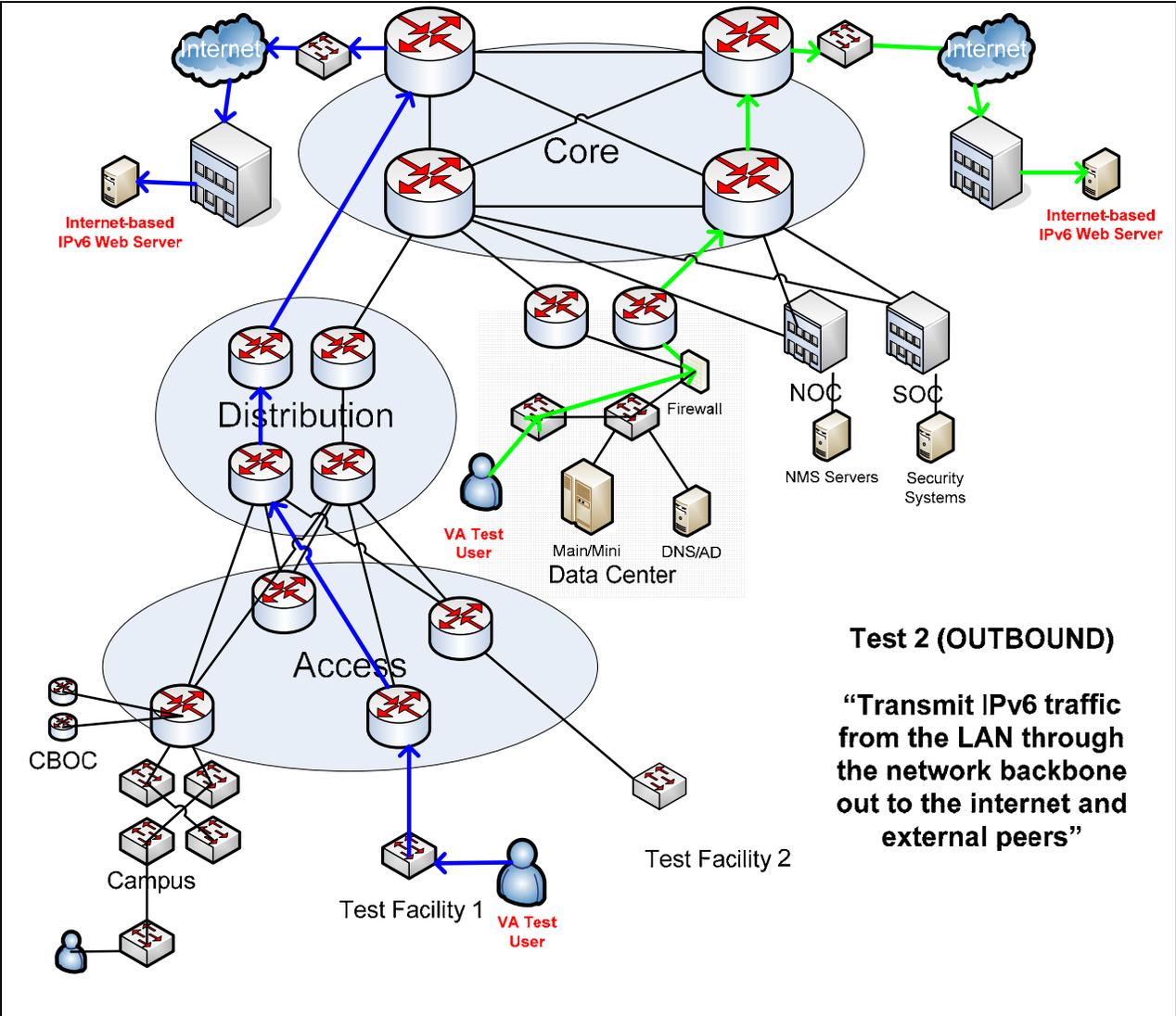
OUTBOUND <i>“Transmit IPv6 traffic from the LAN through the network backbone out to the internet and external peers”</i>	External Location #1 Name: MoonV6 Traffic Direction: Destination Site Type: IPv6 External Web Site	External Location #2 Name: Internet2 IPv6 Partner Traffic Direction: Destination Site Type: IPv6 External Business Partner
VA Site #1 Name: TBD Traffic Direction: Source Site Type: TBD	Test: #1 Test Results:	Test: #1 Test Results:
VA Site #2 Name: TBD Traffic Direction: Source Site Type: TBD	Test: #1 Test Results:	Test: #1 Test Results:
VA Site #3 Name: TBD Traffic Direction: Source Site Type: TBD	Test: #1 Test Results:	Test: #1 Test Results:

Proposed Tests

1. Access an external Web page using a client with a native IPv6 stack.

Success Criteria

1. The Web site displays.
2. The Web site notes that the client IP address being used is an IPv6 address from the VA assigned IPv6 address block.



4.3 Test Case 3 - Internal

INTERNAL <i>“Transmit IPv6 traffic from the LAN through the network backbone to another LAN or another node on the same LAN”</i>	VA Site #1 Name: TBD Traffic Direction: Destination Site Type: TBD	VA Site #2 Name: TBD Traffic Direction: Destination Site Type: TBD	VA Site #3 Name: TBD Traffic Direction: Destination Site Type: TBD	VA Site #4 Name: TBD Traffic Direction: Destination Site Type: TBD
VA Site #1 Name: TBD Traffic Direction: Source Site Type: TBD	N/A	Test: #1, #2 Test Results:	Test: #1, #2 Test Results:	Test: #1, #2 Test Results:
VA Site #2 Name: TBD Traffic Direction: Source Site Type: TBD	Test: #1, #2 Test Results:	N/A	Test: #1, #2 Test Results:	Test: #1, #2 Test Results:
VA Site #3 Name: TBD Traffic Direction: Source Site Type: TBD	Test: #1, #2 Test Results:	Test: #1, #2 Test Results:	N/A	Test: #1, #2 Test Results:
VA Site #4 Name: TBD Traffic Direction: Source Site Type: TBD	Test: #1, #2 Test Results:	Test: #1, #2 Test Results:	Test: #1, #2 Test Results:	N/A

Proposed Tests

1. Run PING and traceroute to an IPv6 address on a client using a client with a native IPv6 stack.
2. Using FTP, transfer data between two clients with native IPv6 stacks.

Success Criteria

1. PING responds.
2. Traceroute responds and shows the expected path.
3. File transfer completes.
4. File transfer time is within 20% of an equivalent IPv4 transfer.

