Application Visibility and Control for IPv6

Why Should I Care?

As a result of the increasing trend of IT consumerization, IT departments are seeing an increased amount of employee-provided or guest devices on their networks, including laptops, smartphones, and tablets.

These devices typically run operating systems that support IPv6 by default and in fact prefer to communicate with IPv6 where possible, using tunneling in certain circumstances.

That is not a cause for alarm, but corporate IT departments need an explicit strategy to integrate IPv6 endpoints on their networks in order to maintain their security policy even if they are not running IPv6 yet.

In addition, IT departments need granular visibility into IPv6 applications and traffic so that they can better prioritize the users/applications. Having deeper visibility into applications running on the network significantly helps cut down the troubleshooting time and efforts.

Who Needs It?

Enterprises with IPv6-enabled employee-provided or guest devices on their network.

What Is It?

Devices running modern operating systems, including laptops, smartphones, and tablets, support IPv6 by default and will attempt to use IPv6 when possible. For example, a Windows 7 device can tunnel IPv6 over IPv4 using a number of methods (6to4, ISATAP, Teredo) to reach IPv6 destinations. Today, hosts should try to use tunnels only if a destination is not reachable natively over IPv6 or IPv4, but older OS versions may use tunnels more aggressively. The Cisco® App Velocity Borderless Network service allows you to identify and classify IPv6 traffic on your network, even if the traffic is encapsulated in a tunnel.

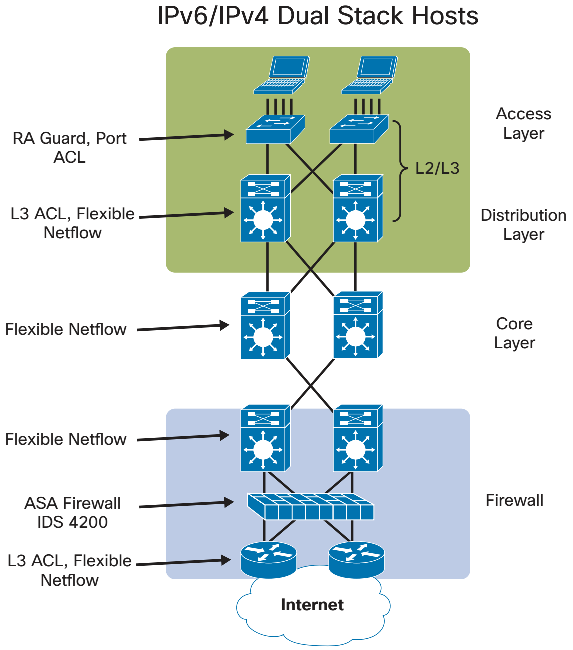
Benefits

Get visibility into IPv6 traffic in your network.

Maintain your security policy when IPv6-capable employee-provided or guest devices connect to your network.

This functionality can be turned on even if the core network or IT-issued devices do not themselves run IPv6.

Cisco Solution for IPv6 Application Visibility



The Cisco App Velocity Borderless Network service provides visibility and control of applications running on the campus or branch network.

App Velocity brings together key technologies embedded in our routing switching products and overlay products to provide end-to-end visibility into IPv6 traffic. Some of the key information that IT administrators now have access to includes:

- Detection of IPv6 endpoints
- Frequently used tunnels that transport IPv6 over IPv4
- Analysis of traffic volumes (bandwidth, sites, VLANS, and so on) for IPv4 and IPv6

The key embedded technologies of App Velocity that are used for IPv6 visibility and control are NetFlow, access control lists (ACLs), Network-Based Application Recognition (NBAR), quality of service (QoS), and special rules on intrusion detection/prevention systems. Cisco Prime™ Network Analysis Module (NAM) provides the management capabilities for analyzing and presenting IPv6 information.

NetFlow is a technology used to collect information about the data flows in a network. It can identify traffic that is being automatically tunneled as well as native IPv6 traffic. NetFlow can give administrators a better view of the initial use of the new protocol, including the ability to assess traffic volume and patterns, variation from IPv4, top talkers, and more.

NBAR can be used to identify and classify IPv6 tunnels to allow the appropriate level of service to be provided for this traffic.

Administrators may want to go further than simple visibility and control the tunneled traffic entering and exiting their network. The Cisco ASA Firewall can be used to implement such security policies, for example, to deny IPv6 automatic tunneling mechanisms and to permit everything else.

The existing intrusion detection and prevention systems (IDSs/IPSs) can also be used to identify IPv6 traffic that might be flowing in a network. Cisco IDS appliances that run software release 6.2 or later can be used to detect native IPv6 traffic and tunneled IPv6 traffic.

Solution Components

Catalyst® 6500, 4500 Series running Cisco IOS® Software

Cisco Firewall ASA 5500 Series

Cisco IDS 4200 Series Sensors

Cisco ISR G2 running Cisco IOS Software

Cisco ASR 1000 running Cisco IOS Software

Cisco Prime Network Analysis Module

Cisco Flexible NetFlow, Enhanced NBAR

© 2011 Cisco Systems, Inc. and/or its affiliates. Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1007R)