

MOVING TO IPv6 WITH REDSEAL

The move from IPv4 to IPv6 is a challenging one, requiring changes to all aspects of your IP infrastructure. RedSeal and the network knowledge it provides can help ensure your transition is a smooth one.

IPv6 AND REDSEAL TODAY

RedSeal can help you identify which parts of your network have been configured for IPv6.

Specifically, RedSeal can:

1. **Locate interfaces in Layer 3 devices that have IPv6 configured**
2. **Validate whether any of those interfaces have an ACL on them**
3. **Identify IPv6 interfaces on perimeter devices**
4. **Identify IPv6/IPv4 interfaces where tunneling may allow unintended data loss**

LOCATE LAYER 3 DEVICES WITH IPv6

Several major service providers are using RedSeal to discover which of their network devices have IPv6 configured. As their network teams implement IPv6, compliance teams need to know where IPv6 has been introduced. Because RedSeal creates a model of your network, including the detailed configurations of all Layer 3 devices, it can identify interfaces that have been configured for IPv6. This information can then be used to configure network scanning products, reducing the time it takes for a thorough scan of deployed IPv6 systems. Compliance teams have really appreciated this, since the alternative, polling-based scanning of the entire IPv6 address space, could take as long as 5 years.

VALIDATE THAT IPv6 INTERFACES HAVE APPROPRIATE ACL

Once you identify interfaces that allow IPv6 traffic, the next step is to ensure that the appropriate access and controls have been configured. RedSeal's knowledge of Layer 3 configurations allows it to inspect your actual access and controls, and identify devices that have IPv6 interfaces and no ACL defined. These could create unintended access paths through that device and expose exploitable areas on your network.

MOVING TO IPV6 WITH REDSEAL

IDENTIFY IPV6 INTERFACES ON THE PERIMETER

RedSeal can also identify perimeter devices that have IPv6 configured. This has been particularly important to our service provider customers, since auditing requirements require that they know their IPv6 perimeter and are monitoring access controls. RedSeal does this by filtering the IPv6 interfaces that lack appropriate ACL controls to identify those with perimeter access.

IDENTIFY EXPLOITABLE PERIMETER ACCESS PATHS WITH TUNNELED IPV6 TRAFFIC

As organizations move through this transition, they have to keep their IPv4 networks secure and control IPv6 utilization. Transition technologies such as tunneling (Microsoft Teredo, 6in4, 6to4, and others) allow IPv6 traffic to traverse IPv4 networks. This can be a security challenge, as 6in4 tunneling, along with IPv6's standard encryption, can be used to smuggle information outside a network. RedSeal can monitor IPv4 perimeter security controls and identify gaps in access controls that would allow tunneled IPv6 traffic.

SUMMARY

RedSeal supports your move from IPv4 to IPv6 by helping to continuously monitor your network and your progress. RedSeal works with all major infrastructure providers so you can fully enable the security benefits of IPv6 on your network, while continuing to improve your overall security posture as you make the transition. For detailed information on how RedSeal can help ensure a successful IPv6 transition, contact your account representative.