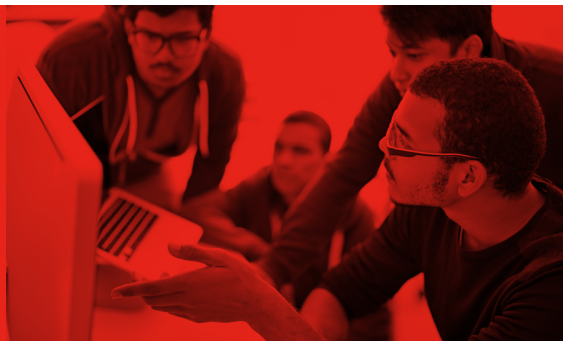
REDSEAL

MODEL AND VALIDATE
APPLICATION-BASED POLICIES



THE CHALLENGE

Back when ports and protocols directly correlated to applications, application traffic was relatively easier to manage. When people mentioned TCP port 25, it was clear they were referring to SMTP. Blocking that port meant blocking the application.

Now, applications are increasingly difficult to identify and rarely play by the rules. Ports no longer equal applications, nor do IP addresses equal users, nor do packets equal content. This change is why security and network administrators want to manage their network security permissions at the application layer rather than by ports or IP addresses.

NEXT-GENERATION FIREWALLS (NGFW)

NGFWs address the evasive applications challenge. They employ deep packet inspection (DPI), a type of data processing that inspects in detail the data being sent over a computer network. They take action by blocking, re-routing, or logging data. DPI is used in many applications, from verifying data formats and checking for malicious code to eavesdropping and censorship. It identifies and classifies traffic based on signatures extracted from the data part of a packet. This allows finer control than classification based only on header information. Many DPI devices can identify packet flows (rather than doing packet-by-packet analysis), so you can control actions based on the entire flow.

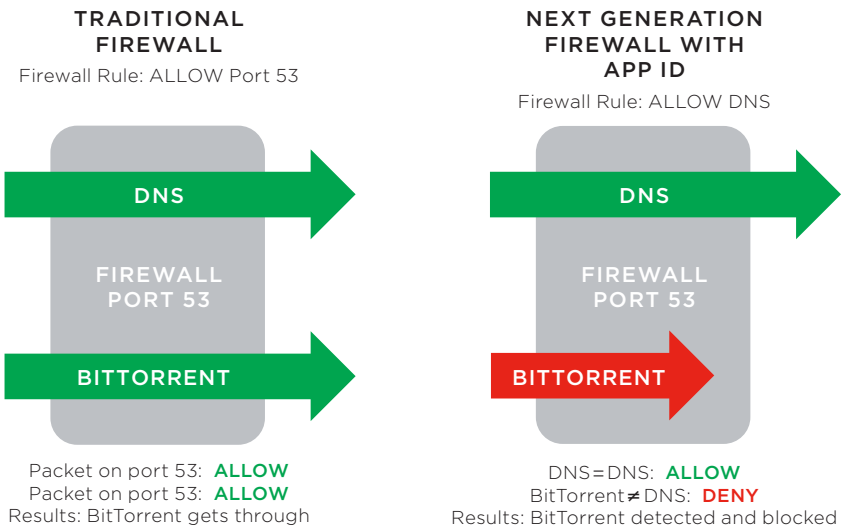


Figure 1: Evasive application on a traditional firewall vs. NGFW with App ID enabled

BENEFITS

- See end-to-end access including Layer 7 application information for both ingress and egress traffic.
  - See where a specific application reaches within your network and if this application poses a threat to you.
  - See where Layer 7 App ID policies are deployed and distinguish between traditional and next-generation firewall deployments.
- Assess risk and compliance, since RedSeal displays permitted applications by name.

SOLUTION OVERVIEW

Enterprises deploying next-generation firewalls can now leverage RedSeal to visualize access and validate policies at the application level (Layer 7), as well as at the networking levels (Layers 2, 3 and 4). Traditional firewall policies are based on the networking level—defined by source and destination IP addresses, ports, and protocol. NGFWs, which are becoming more prevalent in networks, can implement security policies based on the identities of specific applications.

As organizations move away from defining and deploying polices based solely on traditional L2/3/4 characteristics toward allowing or blocking applications, RedSeal validates these policies using the same terminology. For example, RedSeal can validate a "Deny Dropbox" or "Allow WebEx" policy that has been applied to specific addresses, or across all ports and protocols.

No other security, network modeling or cyber risk scoring product provides this level of visibility, understanding and validation of an organization's security posture. With this level of visibility within and between their network environments (physical assets, private and public cloud), teams can understand and prioritize incidents and vulnerabilities wherever they are.

With RedSeal's network modeling and risk scoring platform you can now:

- Query to understand where an application can reach anywhere within your network.
- Model all access paths based on Layers 2-4 and Layer 7 and across public cloud and SDN.
- Validate network segmentation based on Layers 2-4 and Layer 7 and across public cloud and SDN.
- See firewall rules in their entirety—including Layers 2-4 and Layer 7.
- Understand and prioritize vulnerabilities based on network and application access paths.

Figure 2: Access details that include L7 App ID information