WHITE PAPER

IDG
INTERNATIONAL DATA GROUP

Five Key Ways to Increase Network Security

Why enterprises need to take a smart approach to DDI (DNS, DHCP, IP Address Management) to protect their infrastructure

Enterprises have always placed demands on their networks, but today's demands are more complex and more central to meeting business objectives. The need to interconnect multiple technical solutions in support of business-critical requirements only exacerbates the situation. If an enterprise didn't have a rock-solid foundation for its network before, it's going to need one now more than ever.

Part of the increased demand comes from the shift toward more centralized data centers. Enterprises are consolidating servers in virtualized data centers, taking advantage of the reduced costs of hardware and management. The booming bring-your-own-device (BYOD) trend also contributes to new demands on the network. Enterprises want to save money by subsidizing the cost of mobile devices, which means giving employees anytime, anywhere access to data. And of course, a high proportion of these communications—especially when enterprises factor in offering increased data center access to partners, suppliers and customers—run over the Internet.

What do all these communications have in common, besides their ongoing and escalating demands on the network? Security. While IT has to make the data center available and the network reliable, it must also ensure that communications and data are secure. Companies have the option of applying security measures in each of these areas—the data center, mobility and the Internet—but they run the risk of overlapping, bifurcated and perhaps wasteful efforts.

An alternative approach that companies are turning to more and more frequently is to apply stronger and more advanced security to the network foundation itself. By providing security through key protocols embedded in the IP protocol— Domain Name Service (DNS), Dynamic

efficient iP™
DEFINING SMART DDI

Host Configuration Protocol (DHCP) and Internet Protocol Address Management (IPAM), collectively known as DDI—enterprises can not only improve security but reduce the effort required within IT to administer it. Consider the following five ways to employ DDI to strengthen and protect your infrastructure. They add up to a smart approach to DDI.

THE DNS FIREWALL CAN PROVIDE INSIDE-OUT PROTECTION . . . ENTERPRISES CAN SET UP THEIR DNS FIREWALL SOFTWARE TO "BLACKLIST" FORBIDDEN WEBSITES.

TACTIC NO. 1: The DNS Firewall

The DNS is responsible for routing requests to specific websites (domains being the word between *www.* and *.com, .org,* etc., in URLs). As a result, the DNS firewall is a key weapon in the fight for network security, protecting against malware coming in and against employees going out to sites deemed inappropriate.

Let's start with the outside-in method. Some malware programs establish connections through DNS, going outside the network to download harmful programs or communicate stolen information. This typically includes very sensitive information or confidential data including passwords. The password is then used to access, for example, a cloud-based application. Using the DNS firewall, enterprises can track these efforts and stop them before the infected device can transmit inappropriate information or install dangerous programs by blocking the DNS request. IT can then use the DNS firewall to identify the infected device and where it is connected on the network, so that the malware can be deleted.

On the flip side, the DNS firewall can provide inside-out protection as well. Enterprises can set up their DNS firewall software to "blacklist" forbidden websites. These could be anything from Facebook or YouTube to sexually explicit sites. Of course, the DNS firewall software should also be flexible enough to accommodate requests from specific employees for access to certain sites. For instance, sales employees may want to be able to see competitors' YouTube postings; the human resources department may want access to LinkedIn; and the marketing department may need to use Facebook to track *likes* registered in campaigns.

TACTIC NO. 2: DNS Best Practices

A security strategy is never static. Too much is always changing within the network: traffic, loads, even updates from the Internet Systems Consortium (ISC). That's why DNS best practices start with a secure and reliable architecture.

Deploying a secure architecture doesn't mean configuring just one server. With DNS, there is a primary server that communicates information to other (secondary) servers on the network. Unless these connections are configured appropriately and then updated consistently and accurately, architecture security may be at risk. At the same time, if hackers can identify the primary server, the DNS service is exposed to the risk of a DoS attack, which would result in data corruption.

Enterprises must deploy two best practices in this area. One is to create what is known as a "stealth" DNS architecture that hides the identity of the primary server. This makes it much harder for a hacker to hijack that server and strongly mitigates the risk of data corruption. Another method is to use a load balancer from a network vendor. Load balancing provides two advantages: scalability by spreading network traffic among all servers, and an additional level of protection for the primary server by obscuring its location within the overall footprint of the architecture.

Another elementary but still very important best practice is to ensure that the enterprise's servers are running the latest versions of the DNS protocols. These updates come as frequently as every month, on average. If servers aren't updated, they aren't protected. Enterprises need to ensure that all servers are updated consistently to provide the best protection. Doing this manually, however, drains IT resources, so it's best to employ an automated mechanism. That way, IT isn't leaving some servers unprotected due to a laborious update schedule.

Here's another time-consuming IT effort: making sure that all application ports are identified and closed when not being used. Increasingly, companies are relying on automated appliances to ensure that ports are closed not only at the application level, but also at the operating system level for the highest degree of security.

Finally, enterprises are beginning to take advantage of the security protocols built into DNS itself, known as Domain Name System Security Extensions (DNSSEC). This is an especially important practice as companies exchange sensitive information with business partners. Hackers have been known to employ a so-called "man in the middle" offensive, which hijacks information from one server intended for another. DNSSEC addresses this problem by configuring a key on each server to authenticate that information is coming from a trusted source and has not been corrupted. To keep communications flowing smoothly, enterprises can automate the signature mechanism so that secure data gets to its destination faster.

TACTIC NO. 3: Deploy a Consistent IP Topology

As enterprises increase their global footprint, deploying a consistent IP topology becomes even more important. One way to ensure the integrity and consistency of the IP network foundation is to unify management of DDI, virtual LANs (VLANs) and network interfaces. There are several reasons for applying this tactic.

A UNIFIED MANAGEMENT APPROACH ENABLES THE ORGANIZATION AND SEGMENTATION OF NETWORK FLOWS TO INCREASE INFRASTRUCTURE SECURITY.

IP address and VLAN management are profoundly related. A unified management approach enables the organization and segmentation of network flows to increase infrastructure security. This means that the enterprise can accommodate not only current IP transmissions, such as traditional data and VoIP communications, but also any new ones that it might add, such as video cameras and other sensors. With that, it follows that IP and VLAN plans have to be designed and deployed collaboratively, eliminating the risk of misconfiguration and strengthening the network security foundation.

Device and network interface naming and deployments must also be part of the process of truly controlling IP topology design. As an example, the management of the relationships between IP resources enables the precise definition of switches, ports and VLANs to which a server is connected on the network and with its associated IP addresses and names. This end-to-end network design approach provides unprecedented efficient control and accurate visibility of the infrastructure deployment, ensuring global IP topology consistency for higher security.

Another reason for applying consistency to the IP topology: Once enterprises have established templates of subnets aligned with the VLAN configurations, they can replicate that template on new sites. That means they can expand faster if business demands it, while maintaining consistent security structures.

TACTIC NO. 4: Policy and Reconciliation Management

Policy and reconciliation management builds on the concept of a consistent topology for even greater efficiencies in security. By following consistent policies, IT can achieve a high level of granularity. That may seem rigid, but it aids greatly in security. For instance, IT can dedicate subnets to specific kinds of devices and services (VoIP, security cameras, even manufacturing equipment) with predefined VLANs. That way, if someone intentionally or unintentionally tries to add an unauthorized device to a particular subnet, or to an unauthorized port on a switch, the attempt is immediately obvious. Today, when it's astonishingly easy for employees to add Wi-Fi devices in their office, it's important to be able to identify such devices.

An intelligent network reconciliation solution identifies devices and tracks IP and MAC address port connections on the network. It provides comprehensive visibility of network resource deployment and usage, assuring that only authorized devices are correctly deployed within the infrastructure. The more obscure connections in an infrastructure, the more vulnerabilities hackers can exploit. Implementing strict policy and reconciliation processes helps IT identify unknown devices on the network and deployment attempts that do not comply with the defined standard.

TACTIC NO. 5: Captive Web Portal

Increasingly, IT is using the concept of a captive Web portal to balance the twin demands of user access and network protection. This is especially helpful in situations where authenticated users may be signing on with different devices (this may happen, for instance, in academic situations where students or researchers may be using different computers in offices or libraries).

Here's how it works: When known users sign on with unknown devices, the system redirects the requests to the Web portal so that users can answer questions to authenticate their identity. The system then authorizes the DHCP server to allocate IP addresses on the appropriate VLAN, thereby linking previously unknown devices to known users so that they only get redirected once. Because the portal is self-service, it offloads significant amounts of work from IT regarding authentication of new devices.

EFFICIENTIP HAS DEVELOPED A LINE OF NETWORK SECURITY APPLIANCES THAT SUPPORT IT'S EFFORTS TO BOTH SIMPLY AND SOLIDIFY IT SECURITY.

How EfficientIP Helps

By implementing these tactics, IT departments can boost their security strategy immediately. But keep in mind that having multiple tools to handle all of these activities abrogates the efficiencies that come from a single tool that can effectively automate so many of these IP-based activities. As noted in our previous white paper, "Strengthen the Foundation of Your Network," EfficientIP has developed a line of network security appliances that support IT's efforts to both simply and solidify IT security.

In its SOLIDserver appliance, EfficientIP offers the following key features as time-saving capabilities:

DNS FIREWALL: This comprehensive DNS security solution proactively prevents new attacks. It protects the SOLIDserver appliance and other Linux-based devices within the DNS infrastructure by detecting and blocking malware activity and identifying infected devices.

STEALTH DNS ARCHITECTURE DEPLOYMENT AND MANAGEMENT AUTOMATION: With the master DNS server masked from every other server, it's impossible for a hacker to identify and infiltrate the DNS service. EfficientIP offers the SmartArchitecture™, a unique technology to intelligently simplify and automate the design, deployment and management of a stealth DNS architecture.

USER MOBILITY CONTROL: For enterprises concerned about BYOD security, the SOLIDserver appliance incorporates Captive Web Portal & Device Connection Tracking. This lets IT temporarily isolate unfamiliar devices until it can confirm that the users are authentic and authorized to bring new devices online.

SIGNATURE MECHANISMS: The EfficientIP appliance lets IT quickly create a template through which new networks and VLANs can be deployed, reducing time to productivity for new or reconfigured groups or divisions.

POLICY MANAGEMENT: SOLIDserver lets IT set up reconciliations as granular as necessary to ensure that devices and users adhere to established policies.

In creating a secure IP network, it's important to have a tool that helps with all phases of network deployment. SOLIDserver provides IT with an appliance that brings extensive automation to designing, configuring, deploying and managing the network. ■