Domtar Centralizes Authentication and Secures Applications with F5 Solution

Customer: Domtar

Products:

- Application Security Manager
- Access Policy Manager
- Local Traffic Manager

Benefits:

- Consolidated authentication procedures increase control
- Layered solution delivers defense-in-depth across the network
- Centralization of certificates simplifies management
- Virtualization streamlines provisioning of QA environments

Challenges:

- IT team needed to implement centralized authentication and SSO
- Business required layer 7 protection for web applications
- SSL certificate management was labor-intensive
- Developers requested test environments

Business Challenges

Domtar is a paper and packaging company that designs, manufactures, markets, and distributes a wide variety of fiber-based products, including business papers, specialty and packaging papers, and personal hygiene products. With data centers in Canada, the United States, and Europe, Domtar operates a broad production and distribution network, all supported by the IT department.

Domtar has been an F5 customer for many years, having first deployed F5 BIG-IP Local Traffic Manager (LTM) when they had to switch to a new version of Microsoft Exchange and needed the hardware load balancers to optimize the implementation. “Before F5, we didn’t have a smart and flexible load balancing capabilities or a high availability solution,” says Domtar Infrastructure Systems Analyst Pascal Innocenzi. “Just having BIG-IP LTM solved a lot of problems.” Today, Domtar uses BIG-IP LTM to ensure the high availability of most of its internal and external applications.

At the same time, Domtar had other challenges it needed to address. The IT department needed a way to manage access to the company’s internal network, and differentiate the levels of access granted to internal employees and external vendors or contractors. Moreover, Domtar wanted to be proactive about application security, and implement a comprehensive solution that could protect the company’s external applications and keep its internal network safe from attacks.

Furthermore, the company was already looking toward the future, and the possibility of leveraging other components of the BIG-IP platform. “We initially adopted F5,” Innocenzi says, “with the idea that we would expand our other activities to make further use of the BIG-IP platform.”

Solution

And expand they did, bringing BIG-IP Access Policy Manager (APM) and BIG-IP Application Security Manager (ASM) online in the subsequent years. The organization now relies upon BIG-IP APM to control access to its internal network and streamline single sign-on (SSO) procedures across its network. In addition, Domtar deployed BIG-IP ASM to protect its external web applications. Domtar’s layered security solution now leverages BIG-IP APM for centralized authentication, BIG-IP LTM for SSL offload, and BIG-IP ASM as the layer 7 firewall.

Flexibility is a touchstone for Domtar. The IT department employs a number of F5 iRules to customize the interception, inspection, transformation, and direction of inbound and outbound application traffic. For example, the team put an iRule in place that empowers BIG-IP APM to grant different levels of access to an internal SharePoint resource based on the URL a user is requesting access from. “This

allows us to differentiate between internal users and contractors or vendors requesting access," says Innocenzi.

Domtar took advantage of F5's flexible licensing and purchased the Best Bundle, which gives the enterprise the flexibility to expand and scale its solutions as their business evolves. "For instance, we had a web filtering issue a few years ago that I was asked to address," Innocenzi remembers. "If we'd had the Best Bundle at the time, I could have solved the problem in minutes."

Innocenzi says that the flexibility and power of the BIG-IP platform have made a huge difference in the IT workload. "Having the BIG-IP platform in our data centers has really simplified my job, as well as the job of application owners companywide."

Benefits

Domtar deployed a comprehensive F5 solution that allowed the organization to centralize authentication procedures and control access to the internal network by external users. In addition, Domtar now enjoys layered defense from application attacks, simplified SSL certificate management, and a streamlined process for provisioning development environments.

Centralizes authentication for internal and external users

Domtar has centralized authentication and rolled out an SSO strategy that is flexible enough for internal and external users. "We deployed BIG-IP APM because we needed a way to limit the access to internal resources from external partners," says Innocenzi. Now, Domtar has a handful of applications that are externally accessible and the company relies upon BIG-IP APM to control access to them all. "With its capability to handle complex and flexible policies," Innocenzi says, "BIG-IP APM was the solution for everything."

Domtar also used BIG-IP APM to manage SAML federation for their cloud-based applications and partners. The IT department was able to test and deploy a SAML Identity Provider (IdP) in a matter of hours. "And now that it's set up," says Innocenzi, "we plan to use the same SAML IdP for our other partners in the cloud."

Defends against application attacks

The enterprise's layered approach to security involves authentication, a comprehensive SSL strategy, and layer 7 protection through BIG-IP ASM. And with all the traffic passing through F5 appliances, Domtar has an end-to-end security solution that ensures its critical web applications remain highly available, while protecting the enterprise network from a variety of attacks. Again, the ability to script customized policies has allowed the IT department to take full control of company security. "We've really appreciated the flexibility of our security solution," says Innocenzi.

Simplifies SSL certificate management

Managing Domtar's SSL certificates had always been a time-consuming and labor-intensive process. "Before we had BIG-IP LTM," Innocenzi says, "we didn't have a proxy, so clients connected directly to the web servers. Now, anyone who needs to access an internal service goes through a central point of authentication."

This consolidates and simplifies the management of the enterprise's SSL

certificates, because they're stored all in one place. "It's been a great improvement for us," says Innocenzi. In addition, BIG-IP LTM allows Domtar to offload SSL certificate-verification tasks from client and server systems, improving the performance of their applications.

Speeds deployment of QA and development environments

Domtar has an active development team that often requests IT to provision test environments. "In the past," Innocenzi says, "if we wanted to leverage another BIG-IP for development or lab, we had to buy another appliance." Domtar decided to upgrade their hardware appliances to enable F5 Virtual Clustered Multiprocessing (vCMP) technology, a hypervisor purpose-built to host F5 application delivery software.

"We can leverage the vCMP feature to streamline the provisioning of a new development or QA environment," says Innocenzi. Rapidly spinning up new environments allows the company to efficiently test new applications, speed its time to market and ensuring that applications are working well before they are released. Concurrently, the vCMP technology lessens the burden on IT, while simplifying the management of those virtual environments.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | wwww.f5.com

F5 Networks, Inc. Corporate Headquarters info@f5.com	F5 Networks Asia-Pacific apacinfo@f5.com	F5 Networks Ltd. Europe/Middle-East/Africa emeainfo@f5.com	F5 Networks Japan K.K. f5j-info@f5.com