F5 BIG-IP Platform Security

F5 BIG-IP system hardware and software, which use the F5 TMOS operating system, are designed from the ground up to work together to provide total application security.

White Paper

Introduction

Information is the lifeblood of every business's operations. It flows inbound from customers, outbound to the cloud, and from branch offices, to international offices, through the data center, and to the CEO's smartphone. But there's always that one shadowy guy trying to hack his way in.

When creating any security-enabled network device, development teams must fully investigate security of the device itself to ensure it cannot be compromised. A gate provides no security to a house if the gap between the bars is large enough to drive a truck through. Many highly effective exploits have breached the very software and hardware that are designed to protect against them. If an attacker can breach the guards, then they don't need to worry about being stealthy, meaning if one can compromise the box, then they probably can compromise the code. F5 BIG-IP Application Delivery Controllers are positioned at strategic points of control to manage an organization's critical information flow.

In the BIG-IP product family and the TMOS operating system, F5 has built and maintained a secure and robust application delivery platform, and has implemented many different checks and counter-checks to ensure a totally secure network environment. Application delivery security includes providing protection to the customer's Application Delivery Network (ADN), and mandatory and routine checks against the stack source code to provide internal security—and it starts with a secure Application Delivery Controller.

F5's core security team is drawn from all areas of development, and it includes experts with decades of security experience. Its software engineers stay current on the latest threats and vulnerabilities and attend conferences like DEF CON and Black Hat. F5 also considers input about security from its sales and marketing teams, as well as its customers.

Security from the Inside Out

The BIG-IP system and TMOS are designed so that the hardware and software work together to provide the highest level of security. While there are many factors in a truly secure system, two of the most important are design and coding. Sound security starts early in the product development process. Before writing a single line of code, F5 Product Development goes through a process called threat modeling. Engineers evaluate each new feature to determine what vulnerabilities it might create or introduce to the system. F5's rule of thumb is a vulnerability that takes one hour to fix at the design phase, will take ten hours to fix in the coding phase and one thousand hours to fix after the product is shipped—so it's critical to catch vulnerabilities during the design phase. For instance, F5 was adding a mail-relay to one of its products and during testing, it considered an open source mail server product. But for the last ten years, that product averaged one vulnerability per year. F5 ultimately choose a different solution but even that had a list of potential vulnerabilities, such as exposing passwords or the underlying network topology. The sum of all these vulnerabilities is called the threat surface, which F5 strives to minimize. In this example, minimizing the threat surface meant removing unnecessary features of the mail server.

Secure Code from the Start

Eventually, design ends and coding begins. F5, like many companies that develop software, has invested heavily in training internal development staff on writing secure code. But when it comes to software and network exploits, even the smallest mistakes can have huge ramifications. This is where F5 separates itself from the pack. During coding, F5 developers conduct regular code reviews with the security team. One of the most common mistakes found in code reviews is unsafe string functions, which can easily lead to a buffer overflow problem. Another issue is when a program or process tries to store more data in the temporary data storage area than it was intended to hold. Both of these mistakes can cause huge problems; but both are relatively easy to catch.

Next, security testing of the completed code begins. First is penetration testing, in which F5 security staff act as attackers and try to compromise the BIG-IP system. Then fuzz testing begins. The concept is simple: when developers design a program that accepts an input, like a network packet with a pre-defined structure, they assume the input will be correctly assembled—but what if it isn't? The packet length might be too long or short, or the input could have the wrong data. Fuzz testing systematically varies input and observes the results. Some malformed inputs might be handled well, but others might cause the system to crash, and still others could expose a serious vulnerability. For example, fuzz testing has revealed problems with header parsing, in which the headers were too long or contained a malicious format. Penetration testing and fuzz testing make F5 devices as secure as possible against attacks like DoS and even code-based attacks.

F5 also implements a sophisticated third-party scanning application, which analyzes nightly source code for a number of critical flaws. At compile time, the code scanning application looks for flaws such as security bugs and defects, "build breaker" bugs, crashing bugs such as memory leaks and corruption, and unpredictable application behavior introduced by new code. Source code scanning can also find non-fatal flaws such as data integrity issues and performance bottlenecks.

In addition to performing exhaustive internal testing, F5 hires outside firms to conduct "black box" testing in which a third party does application and platform testing "in the dark." This means the firm doesn't have any knowledge of the product beyond what a standard human attacker would have access to (in contrast to source code scanning). Black box testing and analysis can be inserted anywhere in the software development lifecycle, all the way through release. Third parties review code with fresh eyes, which can uncover a subtle vulnerability and add more layers of protection. Once BIG-IP software passes this final test, F5 uses it in its own product environment to ensure it's truly ready for release.

Security testing is time-consuming and a huge undertaking; but it's a critical part of meeting F5's stringent standards and its commitment to customers.

Security in the BIG-IP System

The BIG-IP system has a number of features that provide heightened and hardened security:

- Appliance mode
- iApp Templates
- FIPS
- Secure Vault

Appliance Mode

Beginning with version 10.2.1-HF3, the BIG-IP system can run in Appliance mode. Appliance mode is designed to meet the needs of customers in industries with especially sensitive data, such as healthcare and financial services, by limiting BIG-IP system administrative access to match that of a typical network appliance rather than a multi-user UNIX device. The optional Appliance mode "hardens" BIG-IP devices by removing advanced shell (Bash) and root-level access. Administrative access is available through the TMSH (TMOS Shell) command-line interface and GUI.

Technical restrictions in Appliance mode:

- Access to the Bash shell has been removed.
- Administrative access is limited to the Configuration utility and the TMSH. Administrators can use these hierarchical command line utilities to easily manage and configure the BIG-IP system, and to view statistics and performance data.
- The root user cannot log into the device by any means, including the serial console.
- On platforms that include the Always-On Management (AOM) subsystem, which provides lights-out management for the BIG-IP system, the AOM will not be able to access the host. The AOM will only be able to reset the host using a hardware reset command.

Once Appliance mode has been enabled, it cannot be disabled; rather, customers must obtain a new license from F5 and perform a clean installation of the software. Administrators can verify that a device is running in Appliance mode from the License screen in the Configuration utility of the BIG-IP GUI.

When Appliance mode is licensed, any user that previously had access to the Bash shell will now only have access to the TMSH. The root account home directory (/root) file permissions have been tightened for numerous files and directories. By default, new files are now only user readable and writeable and all directories are better secured.

iApp Templates

Introduced in BIG-IP v11, F5 iApps is a powerful new set of features in the BIG-IP system. It provides a new way to architect application delivery in the data center, and it includes a holistic, application-centric view of how applications are managed and delivered inside, outside, and beyond the data center. iApps provide a framework that application, security, network, systems, and operations personnel can use to unify, simplify, and control the entire ADN with a contextual view and advanced statistics about the application services that support business.

iApps are designed to abstract the many individual components required to deliver an application by grouping these resources together in templates associated with applications; this alleviates the need for administrators to manage discrete components on the network. F5's new NIST 800-53 iApp Template helps organizations become NIST-compliant. F5 has distilled the 240-plus pages of guidance from NIST into a template with the relevant BIG-IP configuration settings —saving organizations hours of management time and resources.

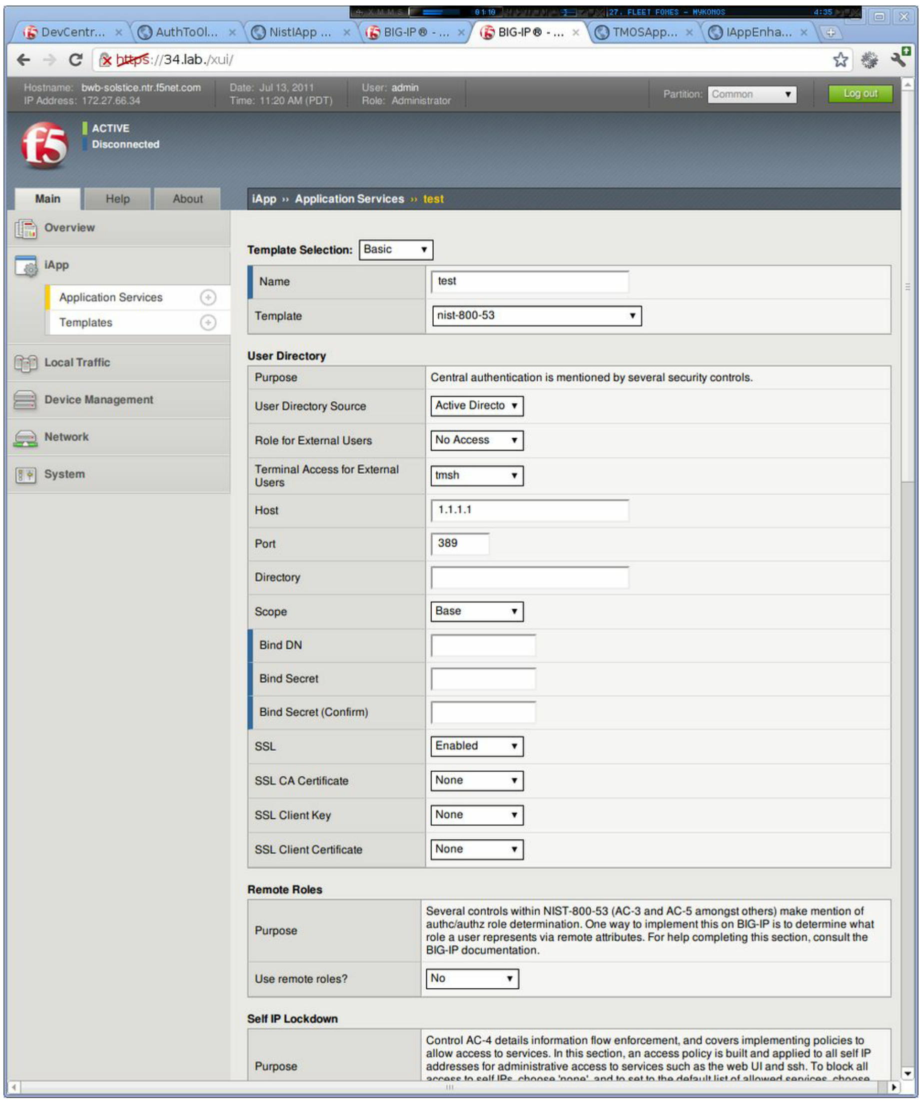

Figure 1: The NIST 800-53 iApp Template

Federal Information Processing Standards (FIPS)

Developed by the National Institute of Standards and Technology (NIST), Federal Information Processing Standards are used by United States government agencies and government contractors in non-military computer systems. FIPS 140 series are U.S. government computer security standards that define requirements for cryptography modules, including both hardware and software components, for use by departments and agencies of the United States federal government. The requirements cover not only the cryptographic modules themselves but also their documentation. As of December 2006, the current version of the standard is FIPS 140-2.

A hardware security module (HSM) is a secure physical device designed to generate, store, and protect digital, high-value cryptographic keys. It is a secure crypto-processor that often comes in the form of a plug-in card (or other hardware) with tamper protection built in. HSMs also provide the infrastructure for finance, government, healthcare, and others to conform to industry-specific regulatory standards.

FIPS 140 enforces stronger cryptographic algorithms, provides good physical security, and requires power-on self tests to ensure a device is still in compliance before operating. FIPS 140-2 evaluation is required to sell products implementing cryptography to the federal government, and the financial industry is increasingly specifying FIPS 140-2 as a procurement requirement. The BIG-IP system includes a FIPS cryptographic/SSL accelerator—an HSM option specifically designed for processing SSL traffic in environments that require FIPS 140-1 Level 2–compliant solutions.

The FIPS card stores the private key associated with a site certificate on a server. It is only used in the initial SSL handshake to securely exchange the SSL session key, which is also known as the symmetric key. Once the client and server establish and exchange a session key, the session key is used to encrypt application data. At this point, the SSL connection no longer utilizes the FIPS card. Instead, a bulk crypto card, manufactured by Cavium, accelerates the SSL encryption and decryption.

Many BIG-IP devices are FIPS 140-2 Level 2–compliant. This security rating indicates that once sensitive data is imported into the HSM, it incorporates cryptographic techniques to ensure the data is not extractable in a plain-text format. It provides tamper-evident coatings or seals to deter physical tampering. The BIG-IP system includes the option to install a FIPS HSM (BIG-IP 6900, 8900, 11000, and 11050 devices). BIG-IP devices can be customized to include an integrated FIPS 140-2 Level 2–certified SSL accelerator. Other solutions require a separate system or a FIPS-certified card for each web server; but the BIG-IP system's unique key management framework enables a highly scalable secure infrastructure that can handle higher traffic levels and to which organizations can easily add new services. Additionally the FIPS cryptographic/SSL accelerator uses smart cards to authenticate administrators, grant access rights, and share administrative responsibilities to provide a flexible and secure means for enforcing key management security.

Secure Vault

It is generally a good idea to protect SSL private keys with passphrases. With a passphrase, private key files are stored encrypted on non-volatile storage. If an attacker obtains an encrypted private key file, it will be useless without the passphrase. In PKI (public key infrastructure), the public key enables a client to validate the integrity of something signed with the private key, and the hashing enables the client to validate that the content was not tampered with. Since the private key of the public/private key pair could be used to impersonate a valid signer, it is critical to keep those keys secure. Secure Vault, a super-secure SSL-encrypted storage system introduced in BIG-IP version 9.4.5, allows passphrases to be stored in an encrypted form on the file system. In BIG-IP version 11, companies now have the option of securing their cryptographic keys in hardware, such as a FIPS card, rather than encrypted on the BIG-IP hard drive.

Secure Vault can also encrypt certificate passwords for enhanced certificate and key protection in environments where FIPS 140-2 hardware support is not required, but additional physical and role-based protection is preferred. In the absence of hardware support like FIPS/SEEPROM (Serial (PC) Electrically Erasable Programmable Read-Only Memory), Secure Vault will be implemented in software. Even if an attacker removed the hard disk from the system and painstakingly searched it, it would be nearly impossible to recover the contents due to Secure Vault AES encryption.

Each BIG-IP device comes with a unit key and a master key. Upon first boot, the BIG-IP system automatically creates a master key for the purpose of encrypting, and therefore protecting, key passphrases. The master key encrypts SSL private keys, decrypts SSL key files, and synchronizes certificates between BIG-IP devices. Further increasing security, the master key is also encrypted by the unit key, which is an AES 256 symmetric key. When stored on the system, the master key is always encrypted with a hardware key, and never in the form of plain text. Master keys follow the configuration in an HA (high-availability) configuration so all units would share the same master key but still have their own unit key. The master key gets synchronized using the secure channel established by the CMI Infrastructure as of BIG-IP v11. The master key encrypted passphrases cannot be used on systems other than the units for which the master key was generated.

Secure Vault support has also been extended for vCMP guests. vCMP (Virtual Clustered Multiprocessing) enables multiple instances of BIG-IP software to run on one device. Each guest gets their own unit key and master key. The guest unit key is generated and stored at the host, thus enforcing the hardware support, and it's protected by the host master key, which is in turn protected by the host unit key in hardware.

Conclusion

F5 provides Application Delivery Network security to protect the most valuable application assets. To provide organizations with reliable and secure access to corporate applications, F5 must carry the secure application paradigm all the way down to the core elements of the BIG-IP system. It's not enough to provide security to application transport; the transporting appliance must also provide a secure environment.

F5 ensures BIG-IP device security through various features and a rigorous development process. It is a comprehensive process designed to keep customers' applications and data secure. F5 hardens its solutions by employing industry-leading safeguards, including:

- Threat modeling
- Code reviews
- Penetration testing
- Fuzz testing
- Black Box testing
- Production testing

The BIG-IP system can be run in Appliance mode to lock down configuration within the code itself, limiting access to certain shell functions; Secure Vault secures precious keys from tampering; and optional FIPS cards ensure organizations can meet or exceed particular security requirements.

An ADN is only as secure as its weakest link. F5 ensures that BIG-IP Application Delivery Controllers use an extremely secure link in the ADN chain.

F5 Networks, Inc.
401 Elliott Avenue West, Seattle, WA 98119
888-882-4447 www.f5.com

Americas
info@f5.com

Asia-Pacific
apacinfo@f5.com

Europe/Middle-East/Africa
emeainfo@f5.com

Japan
f5j-info@f5.com