



# The Milestone Review

MAY 2011

## inside

Secure access for cloud applications ... page 4  
Passing the 'split-handshake spoof' test ... page 6  
Cyber espionage a growing threat ... page 8



Milestone's unique F5 Audit Service provides customers with an in-depth look at the performance of their F5 environments, ranking issues according to risk and providing detailed recommendations.

**C**ompanies rely upon F5 Networks' application delivery controllers (ADCs) to ensure the performance, availability and security of their mission-critical applications across far-flung networks. When F5 units are added to the network at different times, however, configuration variances can accumulate and prevent those units from operating optimally as a group. The implications of this problem increase with the number of F5 ADCs and changing network performance requirements.

Milestone Systems has developed an F5 Audit Service that identifies and ranks issues within the F5 network environment, and provides detailed recommendations as to how to remedy those issues. As the premiere integrator of F5 solutions, Milestone is uniquely positioned to help customers get the highest performance from their F5 appliances.

“We believe our audit process is unique in the industry,” said Tom Marsnik, Operations Director, Milestone Systems. “Because we specialize in several technologies, we are able to access issues both upstream and downstream of the F5s. Our engineers have broad knowledge and deep experience and we have developed an audit program that is extensive and thorough, yet efficient and cost-effective.”

### **Automation Is Key**

Milestone’s F5 Audit Service is available in two levels — Premium and Standard. The Premium Audit is a comprehensive, deep-dive analysis of the F5 network environment, including traffic flows, utilizations and configurations. The Standard Audit provides a high-level snapshot of how F5 ADCs are working and utilized, and identifies areas that need remediation.

“In the Premium Audit, we look at everything in the box, both internal and external. We look at how each unit is handling traffic. We compare configurations to the customer’s standards and industry best practices. We write down every issue that we find in each box and rank it according to risk — critical, serious, moderate and low,” Marsnik said. “We also look at the versions of the units themselves, and identify those that need to be upgraded or replaced.”

Milestone engineers can audit hundreds of F5 devices thanks to sophisticated automation. A special script collects configuration files from every F5 unit within the environment. Engineers examine the configuration files line by line, then input their findings into a program that stores each issue, its ranking and remediation recommendations, and generates a series of reports.

“One of the most challenging and time-consuming aspects of any audit is compiling and sorting the findings of our engineers,” Marsnik said. “So we designed our own proprietary, ‘secret sauce’ application where our engineers can upload their analysis. It stores and ranks everything and kicks out some amazing reports. A particular audit may involve tens of



thousands of objects but we can search all that information and sort it in hundreds of different ways.”

### **Valuable Information**

The reporting tool enables Milestone to provide information that’s very valuable to the customer. The deliverable for each Premium Audit includes an Executive Management Report (high level), Management Report (midlevel) and Engineering Report (detailed view). Each Standard Audit, which normally involves fewer F5 ADCs, includes the Executive and Engineering reports.

**“One of the most challenging and time-consuming aspects of any audit is compiling and sorting the findings of our engineers. So we designed our own proprietary, ‘secret sauce’ application where our engineers can upload their analysis.”**

“The fact that we’ve automated this solution doesn’t mean that the information you’re getting is diminished — just the opposite,” said Marsnik. “Often projects result in information that is so overwhelming it just sits on a shelf and no one ever does anything with it. It’s like a phone book, and all that money you’ve spent is for naught. We wanted to make sure that the information we give back to our customer is in a very understandable format that highlights risks and exactly which issues should be addressed first.”

The Executive Management Report summarizes audit results in a graphical format and provides high-level recommendations as to what steps the organization should take to optimize the F5 environment. The Management Report breaks down each issue according to risk and identifies the F5 devices involved so that IT managers can assign remediation projects to engineers in a systematic way. The Engineering Report provides the engineers with Milestone’s recommended remediation strategy for each problem. Milestone also provides the reports electronically to enable the customer to search and sort the information as needed.

### **Business Benefits**

Automation is also what makes the F5 Audit Program practical. A manual audit that requires a year or two to complete is of little value — much of the information would be obsolete by the time the project is finished. Milestone has reduced months to weeks and created a standardized, replicable solution that is priced based upon the number of F5 units involved.

“Midsize to large companies with 20 or more F5 units can really benefit from Milestone’s F5 audit,” Marsnik said. “Once F5 appliances are up and running they become the heartbeat of the network environment. Unfortunately, few companies have standard policies and processes surrounding F5 installations. Each unit gets configured a little differently, and as a whole they’re not all being used to their maximum potential.”

Marsnik says this not only affects performance but can result in overprovisioning of F5 equipment. Milestone audits have turned up situations where F5 equipment was being utilized at 3 percent or less, whereas a correctly configured unit should handle traffic at about 85 percent utilization. Ultimately, the audit can not only recommend functional improvement of the F5 environment but save money over the long haul.

“We feel it’s important that our customers know how their equipment is performing,” said Marsnik. “Sure, we can sell you more equipment, but our job is to be your partner and ensure that your network is functioning correctly. At the end of the day, Milestone’s F5 audit can give you a complete picture of the current state of your network and help you build a plan to help you achieve optimum performance and availability.”

*To discuss how Milestone’s F5 Audit Service can benefit your organization, contact Milestone Systems toll-free at 866-646-9211 or e-mail [info@milestonesystems.com](mailto:info@milestonesystems.com).*

**milestone**  
systems, inc.

Ensuring High Availability and Network Security  
for Mission-Critical Applications, Since 2000.

BlueCoat



JUNIPER  
NETWORKS



[info@milestonesystems.com](mailto:info@milestonesystems.com)

866-646-9211

[www.milestonesystems.com](http://www.milestonesystems.com)

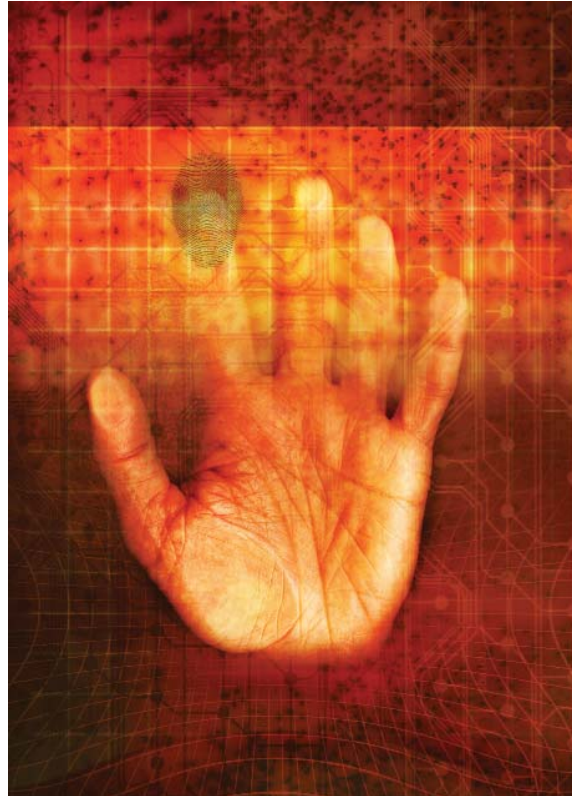
# Secure Access for Cloud Applications

SecureAuth IEP combines strong authentication, SSO and IdM to reduce the risk of unauthorized access, phishing and password attacks, and misuse of portable identities.

**C**loud-based computing dramatically reduces IT expense but doesn't deliver a seamless experience for the end-user or provide strong user authentication to protect applications and data. SecureAuth has brought together everything an organization needs to ensure compliance, increase end-user productivity and fortify security in the cloud. Designed to go from installation to production in days, the SecureAuth Identity Enforcement Platform (IEP) enables transparent access and protection against unauthorized access, phishing and password attacks, and the misuse of an organization's portable identities regardless of where an application resides or how an end-user accesses data.

SecureAuth IEP, the company's flagship product, delivers integrated two-factor authentication, single sign-on (SSO) and identity management (IdM) in a single solution that delivers secure, simple access to multiple applications simultaneously. SecureAuth IEP is configurable to address the requirements for cloud, web and VPN resources with comprehensive authentication services that increase security for on-premises and cloud applications.

"SecureAuth IEP mutually authenticates both the user and the corresponding resource to prevent phishing and password attacks," said Terry Shidla, CISSP, Milestone



Systems. "What's more, SecureAuth's unique browser-based digital certificate eliminates application integration, installation and management of client software, providing strong authentication native to SSO without third-party integration and with no hardware tokens to be managed, lost or stolen."

## Fully Integrated Solution

The integrated SSO services within SecureAuth IEP increase user productivity and reduce the deployment burden on IT. The solution extends desktop log-on to the cloud, providing secure, transparent access to Google Apps, Salesforce.com, ADP and other applications by automatically converting directory identities into application identities. As such, SecureAuth ensures access anytime from anywhere.

Built-in IdM services decrease administrative overhead and reduce help desk costs by enabling users to manage/reset their own passwords. It also supports user self-enrollment based on configurable verification methods. Full integration into Active Directory and other data stores means no data syncing or yet another directory to maintain — authorization is enforced based on role-based access control (RBAC) policies for users and administrators.

“SAML Services in a Box” simplifies integration with Security Assertion Markup Language, OpenID and other open standards for exchanging authentication and authorization data. This “configure don’t code” design provides enhanced federated identity support and enables customers to dial authentication options up or down to meet security requirements.

“We worked closely with hundreds of large global enterprises and partners to ensure we delivered a platform that would meet the needs of any size organization or MSP. The need was well articulated — make every cloud application an extension of the enterprise without compromising security, ease-of-use for administrators, or ease-of-access for end-users,” said SecureAuth co-founder and CEO Craig Lund. “We delivered SecureAuth IEP with integrated SSO, two-factor authentication and IdM to meet these needs while ensuring expandability for future requirements.”

### What’s New in Version 6.0

SecureAuth IEP 6.0 enables mobile platform support by revolutionizing strong authentication for users that have Android devices and iPhones/iPads and access on-premises and/or cloud applications. The downloadable SecureAuth application enables simple, secure setup for strong authentication that enables one-touch access to web and cloud applications. The solution also includes an easily deployed, stay-resident x.509 certificate and one-touch certificate revocation.

Two-factor authentication from the mobile platform back to VPN, on-premises, web and cloud applications is supported on iPhone/iPad, Android, Blackberry, Windows Phone 7, Symbian and more. SecureAuth authenticates the mobile user to the on-premises data store, such as Active

Directory, and delivers VPN digital certificates for Juniper and Cisco clients. End-user self-enrollment and configurable validation options further streamline administrative tasks, and intelligent SSO ensures the right level of authentication by leveraging existing desktop (domain) authentication and/or enforcing web-based strong authentication.

SecureAuth’s multi-tenancy architecture enables access to unlimited web/VPN/SaaS applications or resources from a single SecureAuth appliance. Enterprise multi-tenancy supports diverse requirements of departments and business units within an organization, while SaaS multi-tenancy works across organizations to support service provider models. Customers monitor and administer just one platform to deliver more efficient and effective service and support, including troubleshooting and problem resolution.

“SecureAuth has a technically appealing approach for the next phase of the integration of two-factor authentication and SSO that requires more transparent security and less onerous management overhead.” said Steve Coplan, senior analyst of the Enterprise Security Practice at The 451 Group. “The company’s combination of software-based authentication, enterprise identity propagation and native certificate management is consistent with emerging market requirements for establishing digital trust between service providers and service consumers without adding to management complexity.”

*Streamline secure access to the cloud with SecureAuth and Milestone. To learn more call toll-free 866-646-9211 or e-mail [info@milestonesystems.com](mailto:info@milestonesystems.com).*



## Technical Training



**BlueCoat**



**JUNIPER**  
NETWORKS

[training@milestonesystems.com](mailto:training@milestonesystems.com)  
866-646-9211

See current schedule:  
[www.milestonesystems.com/training/](http://www.milestonesystems.com/training/)

**milestone**  
systems, inc.

# Detecting the 'Secret' Handshake

Palo Alto Networks next-generation firewalls pass the TCP 'split-handshake spoof' test, earning a 'Recommended' rating in NSS Labs Network Firewall 2011 Comparative Test.

**T**hroughout the ages, special handshakes have been used to distinguish insiders from outsiders, friends from foes. Computer networks also use "handshakes" to establish connections. One of the most common is the TCP three-way handshake used in untold numbers of TCP/IP sessions every minute of every day. However, security experts say a little-known exploit called the TCP split-handshake can thwart many network security devices — but not Palo Alto Networks' next-generation firewalls.

In the TCP three-way handshake, a client device sends a message called a synchronization packet, or SYN, to the server. The server acknowledges the client's SYN and sends its own SYN — a combo called a SYN-ACK. The client then closes the loop by responding to the server's SYN with a final ACK.

But in reality the three-way handshake is a four-step process. The client sends a SYN and receives an ACK from the server. The server then sends its SYN and receives an ACK from the client. The three-way handshake is possible simply because TCP networks can combine steps two and three.

That fact paves the way for the TCP split-handshake, or Sneak ACK Attack, in which the server's first ACK is dropped and the client responds to the server's SYN with a SYN-ACK, which the server then acknowledges. This effectively reverses the roles of client and server in the connection, and enables hackers to "trick" the firewall into thinking the connection

can be trusted. Experts say this exploit has been known for about a year.

## Role Reversal

This isn't supposed to work, so few network security devices check for it, allowing a malicious server attacking clients to evade detection. By reversing the logical flow of the TCP connection, the split-handshake confuses intrusion protection, antivirus and other systems that rely upon the direction of network traffic. Testing has shown that some devices become so utterly confused that they respond unpredictably.

NSS Labs, a world leader in independent security product testing and certification, recently tested several firewalls for vulnerability to this exploit. Only one — Check Point — passed the test initially. However, Palo Alto Networks showed rapid response in protecting customers. When test results were posted, the company quickly provided a workaround and within a week posted an update with a permanent fix.

NSS then retested the Palo Alto Networks firewall and confirmed that customers are protected with the new release. As a result, NSS Labs awarded Palo Alto Networks the "Recommended" rating within its Network Firewall 2011 Comparative Test.

The full report including the NSS Labs testing methodology can be found at: <https://www.nsslabs.com/research/network-security/firewall-ngfw/network-firewall-group-test-q2-2011.html>.

## Best All Around

NSS Labs designed the test to focus on the following four areas: security effectiveness, performance, stability and total cost of ownership (TCO). Not only did Palo Alto Networks

pass all effectiveness and stability tests, but only the Palo Alto Networks PA-4020 performed above its stated datasheet performance.

NSS Labs noted that Palo Alto Networks' price/performance is \$10 per protected Mbps, by far the most cost-effective product among the participating vendors — Check Point, Cisco, Juniper, Fortinet and SonicWALL. The closest competitor is 80 percent more expensive, at \$18 per protected Mbps. The only other "Recommended" firewall was \$22 per protected Mbps, or more than twice the cost.

"NSS Labs covered a lot of ground in this network firewall test and we are pleased to have worked with them to retest and subsequently successfully pass all of their tests while still surpassing the performance metrics stated on our datasheet," said Nir Zuk, founder and CTO at Palo Alto Networks. "Given that we're the only firewall in this test that does firewall policy based on application and user, and the only firewall in the test that can decrypt and inspect inbound and outbound SSL, we feel that our security per protected Mbps is more effective, as well as more cost-effective."

"NSS Labs commends Palo Alto Networks for taking the steps to protect their customers," said Vik Phatak, CTO, NSS Labs. "We are impressed with Palo Alto Networks' responsiveness and collaboration during the retesting process and are happy to recommend them."

*To ensure that your systems are protected from the TCP split-handshake spoof, call Milestone Systems toll-free at 866-646-9211 or e-mail [info@milestonesystems.com](mailto:info@milestonesystems.com).*

When You Need

## High Availability & Network Security

Call Milestone Systems



A value-added integrator focused on enhancing networks and serving IT teams in 4 main ways:

- Network Appliances
- Consulting
- Training Classes
- Managed Services

Serving Minnesota, Iowa, Wisconsin, SoDak, NoDak, Omaha, Florida, Georgia, NoCarolina, SoCarolina, Alabama, Mississippi, and Tennessee

952-543-6999 // 866-646-9211

[info@milestonesystems.com](mailto:info@milestonesystems.com)  
[www.milestonesystems.com](http://www.milestonesystems.com)

**milestone**  
systems, inc.

# Cyber Espionage a Growing Threat

**E**nterprises are not taking the threat of cyber espionage seriously enough, and many have not taken adequate steps to prevent an attack, according to a recent study by independent technology analyst Ovum.

“Cyber criminals are graduating from stealing credit cards and banking credentials to targeting corporate plans and proprietary information. They want valuable information such as product and technology blueprints, customer lists or information that can be used to embarrass or disadvantage a victim,” said Graham Titterington, author of the report and Ovum principal analyst. “Almost every organization has sensitive information that would damage it if it were to be leaked out; however, many have overlooked cyber espionage in their preoccupation with preventing the theft of financial data. This needs to change and enterprises need to wake up to the danger posed or risk losing valuable information and having to deal with the consequences.”

Cyber espionage is usually aimed at key individuals within an organization, who are sent “spear phishing” e-mails containing malicious links or attachments that infect their machines. The criminals then use malware to identify assets, decrypt login details and steal the target information.

The report advises enterprises to increase their awareness of cyber espionage, restrict the distribution of sensitive information, vet users who have access to high-value infor-



mation, protect data held on third-party sites and conduct a risk analysis, including mobile devices and removable media.

The report also warns enterprises that holding large amounts of data can increase the risk of falling victim to cyber espionage, and they should look to minimize volumes.

*Milestone has many recommendations for helping you protect your network from cybercrime. Contact us to begin a discussion of your current situation: [ask@milestone-systems.com](mailto:ask@milestone-systems.com).*

**JUNIPER**  
NETWORKS

**NOW!**

Juniper Training for Network  
Architects & Engineers



Learn the full capabilities of your Juniper equipment from highly experienced, “been there” instructors at Milestone Technical Training Classes. Multi-day courses such as:

- ♦ JUNOS software (intro, troubleshooting, or advanced)
- ♦ Advanced Juniper Routing in the Enterprise
- ♦ Configuring Security Threat Management
- ♦ Integrating Juniper Firewalls & VPN's into High Performance Networks
- ♦ And more! Call us for the topic you need.

See current schedule of classes at [www.milestonesystems.com/training](http://www.milestonesystems.com/training) or call Paul Eck, Milestone Training Manager, to discuss your Juniper training requirements. Class can be at our facility or yours.

**milestone**  
systems, inc.

866.646.9211 or 952-767-5142  
[training@milestonesystems.com](mailto:training@milestonesystems.com)