

“What I like about VPN-1 Pro/FireWall-1 is from the start there was a consistent philosophy that has never changed. It has continued to be upgraded to respond to new threats, but the basic technology hasn’t changed.”

*Mr. Tomokazu Nemoto
System Engineer, Tokiwa University Media
and Information Technology Center*



CUSTOMER NAME

Tokiwa University

INDUSTRY

Education

CHECK POINT PRODUCTS

- VPN-1® Pro™/FireWall-1®
- InterSpect™
- SmartDefense™

CUSTOMER NEEDS MET

- Consistent security infrastructure that evolves toward new threats
- Strong perimeter security
- Internal security for wireless LAN

Tokiwa University Relies on Check Point for an Integrated Solution to Campus Network Security

ABOUT TOKIWA UNIVERSITY

Founded as a junior college in 1966, Tokiwa University is a private educational corporation in Japan that now encompasses the entire range of education from kindergarten to graduate school. In May 2005, the university unveiled its new Media and Information Technology Center to facilitate education and research across the campus, as well as offer more effective classes to students. For network security, Tokiwa University relies on Check Point Software Technologies and its VPN-1® Pro™/FireWall-1® and SmartDefense™ solutions.

THE TOKIWA CHALLENGE

Emphasizing the important role of the Media and Information Technology Center, Mr. Masanobu Abe, professor in the department of human sciences and director of the new center, says, “We see corporations investing in the development of leading-edge hardware and software, moving the broadband platform forward. But it seems to me that small- and midsize businesses aren’t taking a strategic approach to developing and using software or other content that makes the most of this advanced platform. One important role of the Media and Information Technology Center is to educate people in Web programming, computer graphics, digital image production, and other digital media information technologies, and then send them into the world to help these smaller companies.”

The center houses a full inventory of digital equipment, including computers, video production studios and equipment, and much more. Consolidated and centralized resources allow information to be shared among departments separated geographically but now connected electronically. This has fostered an environment that facilitates education and research.

In 1995, the university connected to the Internet through participation in SINET (Science Information Network). As the needs of the faculty and students quickly grew beyond Web browsing and email, branching into a variety of other applications, the university faced growing issues of network bandwidth and guaranteed availability. Stating the need to balance security with network expansion and guaranteed availability, Mr. Tomokazu Nemoto, system engineer of the Media and Information Technology Center says, “For us to respond to Internet usage needs, we must be able to expand the network while maintaining its ease of use. And we have

to have an environment allowing free access to the Internet for students, which means we absolutely have to have strong security measures in place.”

THE CHECK POINT SOLUTION

In the year following its connection to SINET, the university implemented VPN-1/FireWall-1. This is the most popular perimeter firewall in the world because it uses INSPECT, the most adaptive and intelligent inspection technology, to provide both network- and application-layer protection.

When a wireless LAN environment was implemented, allowing faculty and students to use their mobile PCs on campus, the university had foresight that those PCs would have insufficient security measures and knew that the network would need protection not only from external threats but internal ones as well.

To resolve these issues, Tokiwa adopted Check Point’s InterSpect™ internal security gateway. InterSpect protects internal networks from personal mobile computers that may not be secure. It incorporates functions to prevent the proliferation of worms and other attacks inside a network, segment an internal network into protected security zones by department, and quarantine infected devices that propagate attacks or worms.

Tokiwa University also keeps ahead of evolving Internet security threats by subscribing to SmartDefense™ Services for real-time updates and security advisories for its Check Point security infrastructure.

THE BENEFITS OF CHECK POINT SECURITY

When Tokiwa University chose FireWall-1 in 1996, two factors were important: The interface was easy to understand—greatly simplifying the deployment and ongoing management of multiple firewalls—and FireWall-1 was software-based, so the university could run it on its existing Unix servers.

Stable foundation for network security

“What I like about VPN-1/FireWall-1 is from the start, there was a consistent philosophy that never changed,” Mr. Nemoto says. “It has continued to be upgraded to respond to new threats, but the basic technology hasn’t changed. What I mean by basic philosophy is that the core of the system monitors and inspects the status of data packets and then applies rules whereby only data necessary for communications is allowed to pass through automatically. To prevent new threats, we implemented SmartDefense Services, which also follows this basic philosophy and is easy to use since it has the same interface.”

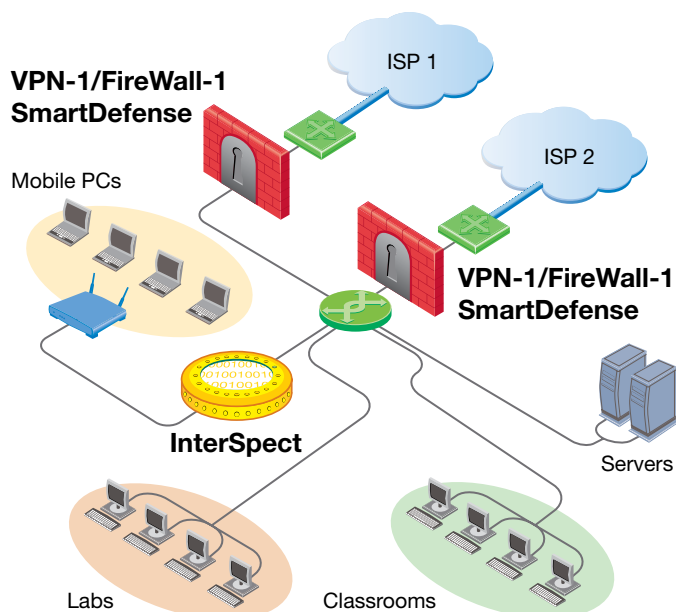
Behind the basic Check Point philosophy that Mr. Nemoto praises, the core INSPECT technology forms a foundation upon which a newer architecture in the form of Application Intelligence™ and SmartDefense has been built. From simple misuse of packets to large-scale attacks, this technology offers thorough protection for an organization’s network.

According to Mr. Nemoto, products from other companies claiming functionality similar to InterSpect seemed to emphasize treating security deficiencies on mobile PCs. “The concept behind InterSpect was more in line with our view that security for mobile PCs is the responsibility of the PC owner, while the network operator has to protect the internal network.” At present, the school restricts personal computer connections to the LAN inside specially segmented areas in the Media and Information Technology Center. However, the plan is to expand the number of areas where students and faculty can connect.

THE FUTURE OF TOKIWA UNIVERSITY

With the completion of the Media and Information Technology Center, the Tokiwa University campus backbone has been upgraded to between 2Gbps and 8Gbps bandwidth, while classrooms and research labs have been outfitted with either 10Mbps or 100Mbps connectivity. At present, the school is in its second phase of construction, implementing gigabit connectivity for research labs around the campus.

“Not a day goes by that we don’t detect some kind of DoS or SQL injection attack or any of hundreds of IP sniffing attacks. But we haven’t incurred any damages, yet, which I believe is a benefit of implementing VPN-1 Pro/FireWall-1 and SmartDefense,” says Mr. Nemoto. “With the new Media and Information Technology Center and the construction of our virtual studio, we see all kinds of traffic over the campus network. It’s important that our network is both robust and secure.”



Tokiwa University uses Check Point perimeter and internal security products for an integrated solution to network threats.

CONTACT CHECK POINT

Worldwide Headquarters

5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-575-9256 | Email: info@checkpoint.com

U.S. Headquarters

800 Bridge Parkway, Redwood City, CA 94065 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com

©2003–2008 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Endpoint Security, Check Point Express, Check Point Express CI, the Check Point logo, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Provider-1, PureAdvantage, PURE Security, the puresecurity logo, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Security Management Portal, Sentivist, SiteManager-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartView Tracker, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, UTM-1 Edge, UTM-1 Edge Industrial, UTM-1 Total Security, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power Multi-core, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm ForceField, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, and the Zone Labs logo are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. ZoneAlarm is a Check Point Software Technologies, Inc. Company. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668, 5,835,726, 5,987,611, 6,496,935, 6,873,988, 6,850,943, and 7,165,076 and may be protected by other U.S. Patents, foreign patents, or pending applications.