Leading International University Squashes Threats from Modern Malware with Palo Alto Networks

"Palo Alto Networks gives us true insight into what's really going on in our network to ensure that risky traffic and activity is blocked. The control, visibility and threat prevention capabilities of the PA-4000 Series are unmatched. The cost was right and the benefits quickly justified the cost."

– Mente Heemstra, Network Specialist, University of Groningen

BACKGROUND

Founded in 1614, the University of Groningen enjoys an international reputation as one of the oldest and leading educational and research universities in Europe. Located in the north of the Netherlands, the university offers degree programs at Bachelor's, Master's and Ph.D. levels in virtually every field, many of them completely taught in English. Research and knowledge, combined with an interdisciplinary approach, form the basis of the school's programs. Research and education at the University of Groningen is internationally oriented, as students from every continent prepare themselves for international career paths. Groningen is an ideal, safe city with a flourishing student life.

FILE SHARING AND MALWARE ON CAMPUS

Approximately 28,000 students study at the acclaimed University of Groningen. The university includes the Medical Centre Groningen (UMCG), and features a state-of-the-art 3D projector room for virtual reality studies. Powered by the IBM Blue Gene/P, the university boasts one of the fastest computers in the Netherlands, with 12,288 processor cores, and 6 Terabytes of memory, delivering 41,78 TFlops performance.

Roughly 8,000 staff conduct research, teach and support students in their educational pursuits at the institution. The school's IT core, consisting of six Cisco 6509s with 10 gigabyte interconnections, and Supervisor 720, support the computing needs of students, faculty and staff.

OPEN ACCESS AND ACADEMIC FREEDOM

As an institution of higher learning, the university's philosophy is to allow each student and employee the freedom to access applications and web sites unfettered by usage policies. "We do not interfere with or block student or staff access to applications, web sites or file sharing, unless something very risky or particularly strange is going on," states Mente Heemstra, Network Specialist for the University of Groningen, who has been managing the university's networking and security infrastructure for decades.

"There aren't any specific application usage policies. We permit all traffic except that identified as unsafe, and simply block malware and other threats to our network."

university of groningen

ORGANIZATION:
University of Groningen

INDUSTRY:
Education

CHALLENGE:
Gain visibility into network to improve security and control while maintaining a policy of application access for all users.

SOLUTION:
Replace legacy firewalls and Intrusion Prevention System (IPS) managing traffic between the university and its Internet Service Provider with Palo Alto Networks PA Series next-generation firewall with IPS for granular visibility of threats and better control of suspect Internet applications.

RESULTS:

- Improved security
- Greatly reduced Mariposa, Conficker and SQL Slammer malware as threats
- Effectively blocked suspect traffic
- Gained granular visibility into the network
- Cost-effective solution

paloalto NETWORKS
the network security company™

"The great thing about the PA-4000 Series is I can easily install it and block all high risk and critical incidents. It actually shows me applications, not just ports, and tells me what a port is used for even though it looks like an HTTP port."

Mente Heemstra
Network Specialist
University of Groningen

Like many schools with large numbers of staff and students, the University of Groningen must balance research needs with network safety. Its open usage approach can make it vulnerable to threats from modern malware. "The malware we see the most on our network are Mariposa, Conficker and the SQL 'Slammer' worm," explains Heemstra. These threats intermittently cause network degradation and hinder the performance of the targeted systems. Peer-to-Peer (P2P) file sharing on campus networks – particularly among students – also exposes the university's network to security risks and copyright infringement issues.

The university did not have an Intrusion Prevention System (IPS), so it blocked traffic by referencing access lists and log files in its core routers. "It was slow and incapable of handling the 2-3 Gbps of traffic that comes into our network," says Heemstra. "To search through this amount of data with this system was very, very slow and cumbersome. It took several hours just to get a traffic report based upon the specifics of a problem."

WHICH SOLUTION ACES THE TEST?

To better secure its network, increase the amount of Internet traffic it could inspect, and accelerate the time it took to do so, the University of Groningen researched available network security and threat prevention solutions on the market. "We wanted something that could provide more network visibility and block suspect traffic at a minimum of 4Gbps – both for IPv4 and IPv6 – while allowing us to maintain an open usage policy," states Heemstra. "The right total cost was also a big issue. I looked at every IPS product on the market before deciding on Palo Alto Networks' PA-4000 Series."

The next-generation PA-4000 Series firewall with IPS enables unprecedented visibility and granular policy control of applications and content – by user, not just IP address – at up to 10Gbps with no performance degradation. The PA-4000 Series isolates and protects data through security policies that are based on the user or group identity from within Active Directory. The user and group identity is then tied directly to a specific application, and the application can then be inspected for threats and unauthorized data transfer. This level of granular control is unmatched by any firewall solution on the market.

The PA-4000 Series satisfied the university's pricing and other criteria. A trial evaluation was arranged and administered by Palo Alto Networks' reseller in the Netherlands, ON2IT. "The evaluation of the PA-4000 Series by ON2IT really illustrated how much uninspected application traffic and malware was on our network," relays Heemstra. "It was very enlightening. With the PA-4000 Series it was easy to clearly see the extent of Mariposa activity, in particular."

Palo Alto Networks' next-generation firewalls are ideal for universities and businesses seeking to prevent modern malware and safely control applications, instead of the block-or-nothing approach offered by traditional port-blocking firewalls. "After looking at several firewalls and IPS products, we chose Palo Alto Networks because of its broad range of capabilities, relatively low price and a positive report by Gartner Group about the PA-4000 Series," relays Heemstra. Convinced, the University of Groningen purchased two Palo Alto Networks PA-5060 firewalls for IPS and threat prevention, replacing its legacy Cisco ASA firewalls and incumbent IPS device.

PREVENTING MALWARE, PROTECTING THE NETWORK

Heemstra has been extremely pleased with the network visibility, security, application control and performance of the PA-4000 Series. "The Palo Alto Networks solution proved its value very quickly," he reports. "We already found and took care of several new bugs. Plus, we eradicated Mariposa botnet traffic from our network."

The university plans to use Palo Alto Networks to secure its IPv6 and IPv4 infrastructure as well. "The beauty of the PA-4000 Series is that it doesn't discriminate between traffic using IPv4 or IPv6," describes Heemstra. "It enables us to see all IPv6 traffic and application-based intrusions in tunnels, and then scan for signatures in applications. We plan to block all IPv6 tunnels that transport traffic (except for true VPN tunnels), to eradicate some threats concerning dual stack systems inside our network. This will allow us to protect Vista Windows machines no matter what kind of traffic they pass."

In addition to providing more performance for the dollar than legacy UTM systems, the PA-4000 Series enables enterprises to accurately identify and control applications by user, scan content to stop threats, and prevent data leakage – all with a single network device. "The great thing about the PA-4000 Series is it actually shows me applications, not just ports," says Heemstra. "Ports can be related to risky traffic, but the Palo Alto Networks box tells me what a port is used for even though it looks like an HTTP port. I can easily install it and block all high risk and critical incidents."

Palo Alto Networks has also been deployed on the school's links to its Internet Service Provider (ISP). "It effectively blocks all unwanted traffic," explains Heemstra. "Moreover, we now have a complete flow collection of all traffic between our network and the Internet. Even though we log nearly 40 gigabytes of data per day, whenever there's a problem we can quickly and easily search the data. This is saving us huge amounts of time."

To protect the servers at the university's Medical Centre Groningen, ON2IT offered the school two feature rich Palo Alto Networks PA-2050 firewalls at an attractive price point. ON2IT's package won out over proposals from several other vendors. "Currently, Palo Alto Networks beats its competitors by delivering good security at the right price," Heemstra states.

"Palo Alto Networks gives us true insight into what's really going on in our network to ensure that risky traffic and activity doesn't happen anymore," sums up Heemstra. "The control, visibility and threat prevention capabilities of the PA-4000 Series are unmatched. The cost was right and the benefits quickly justified the cost."

paloalto NETWORKS
the network security company™

3300 Olcott Street
Santa Clara, CA 95054

Main: +1.408.573.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com