

City of Seattle Improves Application Usage Control Policy and Enforcement with Palo Alto Networks

“Palo Alto Networks has created a new generation of security device that identifies applications – not just ports, protocols and source/destination IP addresses – and enforces policies concerning application usage. The granular visibility and control that Palo Alto Networks gives us has allowed us to re-write and enforce our acceptable application usage policies and protect the city.”

— Michael Hamilton, CISO, City of Seattle

BACKGROUND

The City of Seattle Information Technology Department acts as a service provider to a federated system of 50-odd departments, and is a juncture point for multiple intergovernmental networks. Tasked with managing the applications, networking infrastructure and backbone that supports 10,000 users, while complying with various regulatory requirements, network security is of paramount importance.

APPLICATION AND WEB TRAFFIC CONTROLS

Michael Hamilton, Chief Information Security Officer (CISO) for the City of Seattle, knows a thing or two about information security. The Department of IT is an infrastructure provider to a federated system of local governmental agencies. As a collection of high-value critical infrastructure targets including transportation, public safety and utility systems, the City is exposed to very serious attacks. Nation-states, terrorists, insiders, organized crime – you name it and the City of Seattle sees it every day.

The City of Seattle’s Office of Information Security (OIS) continually evaluates potential solutions to address this unique set of threats. To that end, they sought a solution to address the shift from e-mail attachments to Internet content and applications as primary threat vectors. What was needed was technology to block undesirable applications and control web access. Their goal was to not only control web surfing but to block known malware download sites and stop applications that placed the network at risk and the city in jeopardy of non-compliance. With those criteria in hand, the OIS began evaluating the logical options of IPS and URL filtering solutions. They also decided to look at Palo Alto Networks. The Palo Alto Networks firewall presented unique combination of visibility and control over both applications and web traffic.



ORGANIZATION:

City of Seattle

INDUSTRY:

State and local government

CHALLENGE:

Controlling applications and web access, blocking threats.

SOLUTION:

Palo Alto Networks PA-4020 provided the data required to rewrite and enforce application and web usage policies.

RESULTS:

- Appropriate application usage policies have been re-written and provided to users.
- Network is free of unapproved applications like P2P, IM, and Skype.
- A wide range of malware and application vulnerability exploits are being blocked.

“The network is cleaner, safer and faster. And there is a more detailed policy on what the users should and should not do on the network.”

Michael Hamilton,
CISO,
City of Seattle

ROGUE APPLICATIONS PROBLEM IS WORSE THAN EXPECTED

Within 15 minutes of deploying a Palo Alto Networks PA-4020 in tap mode on a SPAN port to monitor one of his intergovernmental segments, Michael and his team began seeing a wide range of bad traffic traversing the network. The measurements showed a surprising amount of spyware, P2P applications, IM clients, streaming media and a variety of soft phones. The team was shocked, primarily because multiple IDS systems are in use; they were under the impression that their P2P and IM detection was pretty good. Their response was, “we had no idea how bad it was.”

The next step was a delicate one to take. As a service provider to the other networks and agencies, Michael and his team must walk a fine line of control and security versus the other established policies and procedures of all the other departments (technically his customers). For example, the team has little control over which applications were installed on end-user systems in some departments, but are able to implement controls to enforce policy.

RE-WRITE AND ENFORCE ACCEPTABLE USE POLICIES

Rather than act as big brother and clamp down on the traffic and risk customer dissatisfaction, the OIS took a softer approach. They monitored the applications traffic and created reports that were distributed to other departments and affected stakeholders. Those reports opened everyone’s eyes and facilitated an agreement to take action. First they used the data to re-write their acceptable use policy and address the range of applications identified. And then they dialed the control mechanisms up on the applications traffic traversing the network, blocking the bad applications and inspecting the allowed applications in the context of enforcing existing policy. Michael saw it as a win-win scenario. “The network is cleaner, safer and faster. And there is a more detailed policy on what the users should and should not do on the network.”



Palo Alto Networks
2130 Gold Street, Suite 200
Alviso, CA 95002-2130
Main 408.786.0001
Sales 866.207.0077
www.paloaltonetworks.com