Building a Safer, Smarter State Government

State of Oregon safeguards confidential information with Cisco Self-Defending Network solution.

EXECUTIVE SUMMARY

STATE OF OREGON

- **Industry:** Government
- **Location:** Salem, Oregon
- **Number of Employees:** 45,000 employees

BUSINESS CHALLENGE

- Enhance network reliability to keep critical government services available
- Meet state and federal privacy regulations
- Ease network administration

NETWORK SOLUTION

- New firewall system offers intelligent protection and support for secure VPNs for remote offices
- Intrusion prevention tool enables proactive protection from network threats
- Security monitoring system provides an end-to-end view of the network and helps improve threat mitigation
- Subscription service supplies trained engineers to facilitate network design, deployment, optimization and operation

BUSINESS RESULTS

- Standardized platform, together with Cisco management tools, helps reduce network management costs
- Proactive security environment safeguards data and makes administration more efficient

Business Challenge

The state of Oregon is committed to improving the quality of life for all of its citizens. A national model for improving government, the state strives to deliver the highest level of service to its residents. More than 100 agencies are responsible for day-to-day government concerns such as education, public safety, human services, transportation, business, finances, and the environment.

Information technology plays a key role in helping all of these agencies work efficiently, collaborate, and respond to constituents. Traditionally, each organization has been responsible for maintaining its own IT environment. Different systems and staff were dispersed across the state, each using its own business approach. However, this model left the state of Oregon vulnerable to network security issues that could bring government operations to a standstill.

“Some of our agencies had very good security organizations and response, but others were not quite as prepared,” says Al Grapoli, network manager at the state of Oregon. “Any security breach had the potential to spread everywhere, and was difficult for us to identify and isolate.”

To consolidate its dispersed networks and make operations more efficient and manageable, the state launched a new initiative: The Computing and Networking Infrastructure Consolidation (CNIC) project. Security was a top priority for the project, because the state had to meet strict standards to protect private information.

“Our agencies are subject to several different federal and state regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), which governs personal health information,” says Grapoli. “These regulations require us to safeguard information at all of our organizations, from Health and Human Services to the Department of Motor Vehicles, state police, and many other agencies.”

The state of Oregon needed a complete security solution that could provide defense in-depth at all of its office networks. To keep key government services running, the state also sought to make its network infrastructure more resilient and reliable. Since IT staff size was limited, the solution would

have to be easy to manage and maintain.

> **"When we build a security environment that is flexible, manageable, and layered, we can handle any new challenges that may appear. Our Cisco solution definitely gives us this capability."**
> **—Al Grapoli, Network Manager, State of Oregon**

Network Solution

In 2005, the State of Oregon began work on the CNIC initiative, which was based on a new converged data center featuring a Cisco® network. The Cisco Self-Defending Network was a critical component of the CNIC project in that the new data center clearly needed to protect highly confidential information, comply with government regulations, and be flexible to meet the diverse needs of all of its agencies.

"To achieve a comprehensive approach to security, we looked at a variety of products and architectures. The Cisco solution delivered the highest level of flexibility, and enabled us to build multiple layers of security. It really fit into what we needed to do, because each agency required a specific level of security for its operations," says Grapoli.

As a first step in implementing its new security architecture, Grapoli and his team converted its existing repertoire of Cisco PIX Firewalls to Cisco ASA 5500 Series Adaptive Security Appliances at more than 60 remote offices. More robust and flexible than the Cisco PIX Firewall, the Cisco ASA 5500 Series Adaptive Security Appliances are purpose-built security solutions that can easily scale to meet the state of Oregon's changing needs. A core component of the Cisco Self-Defending Network, the Cisco ASA 5500 Series provides proactive threat defense that stops attacks before they spread through the network, controls network activity and application traffic, and delivers both IPsec and Secure Socket Layer (SSL) VPN connectivity.

"Migrating from Cisco PIX to the Cisco ASA has been straightforward, because we are using the same operating system, yet gaining greater flexibility," says Grapoli. "We haven't had any significant issues migrating; we simply take the rule set from the Cisco PIX and plug it into the Cisco ASA."

The state looks forward to exploring the many unique capabilities of the Cisco ASA 5500 Series, and is already taking advantage of the advanced firewall and VPN capabilities. These robust security features protect the network against unauthorized access and provide secure connectivity for agency employees.

"With the Cisco ASA, agency employees working at remote sites can securely access a wide variety of tools and applications. For example, they can make changes to their employee benefits plan over a secure Web site," says Grapoli.

For end-to-end network protection, the state is deploying a Cisco Intrusion Prevention System (IPS) solution. Using Cisco IPS 4200 Series Sensors, the state can identify, classify, and stop known and unknown threats like worms, network viruses, and application threats.

"Intrusion detection can only go so far in stopping threats, but Cisco's sophisticated intrusion prevention capabilities let us work proactively to discover and eliminate threats early," says Grapoli.

“IPS can stop attacks and intrusions before they can cause any damage on our network.”

To make the most of its security investment, the state needed a way to monitor all of the network’s security devices and host applications to develop an end-to-end view of the network. Using the Cisco Security Monitoring, Analysis and Response System (CS-MARS), Grapoli and his team can use the intelligence in their network to identify, manage, and counter security threats.

Cisco Security Services also played an important role at every stage of the network solution deployment. The state of Oregon subscribes to the Cisco Security Optimization Service which affords Grapoli and his team skilled Cisco engineers to assist with designing, implementing, operating, and optimizing the security architecture.

“Cisco services have provided a tremendous value,” says Grapoli. “We would not have been able to meet our objectives without them.”

Business Results

The new Oregon data center and network have quickly had a dramatic impact on security and management, improving network visibility and reducing threat response time.

“Under our past model, each agency was managing its own network resources,” says Grapoli. “Our Cisco solution enables us to centralize network administration, so we can exercise better control across many agencies—even with our small staff.”

The Cisco solution has also enabled the State of Oregon to standardize its equipment and procedures to manage the network more efficiently and make the best use of employee expertise. “Using a standardized platform lets us avoid the need to support firewalls and other devices from multiple vendors,” says Grapoli. “Trying to manage five different firewalls is difficult.”

CS MARS has played a key role in helping the state safeguard its organization, transforming raw network and security data into intelligence that can be used to fight threats. “CS MARS is a big help in enabling us to capture logging, and review and rapidly respond to threats,” says Grapoli. “Just this past week it helped us discover a new virus. We picked it up quickly and alerted all the organizations that had been impacted by it.”

Cisco Security Services engineers have been actively involved in building the new state of Oregon network. Designed to support every stage of the solution lifecycle, Cisco Services help the State of Oregon to continually assess how well its technology aligns with its business needs.

“Working with Cisco Services, we have initiated a six-month analysis of our WAN and LAN,” says Grapoli. “We will evaluate all of the network devices in use, and determine how they impact the overall health and security of the network.”

With a comprehensive Cisco Self-Defending Network in place, Grapoli is confident that the state of Oregon can comply with government requirements today, and tackle new security issues that emerge in the future.

“When we build a security environment that is flexible, manageable, and layered, we can handle any new challenges that may appear,” he says. “Our Cisco solution definitely gives us this capability.”

Next Steps

Grapoli and his team have already begun taking steps to further safeguard the state’s data center with new security solutions. Cisco Security Agent software will reside on 1000 servers. Ideal for

performance-sensitive server environments, Cisco Security Agent provides proactive protection against threats that have not been seen before, as well as emerging threats. Cisco Security Agent will also help reduce the need for emergency system patching when new threats arise.

“The technicians that support our desktops believe that Cisco Security Agent can help us save administrative time in patching, freeing them to concentrate on other job priorities,” says Grapoli.

To make sure that any device using the network conforms with security policies, the state is also installing Cisco NAC Appliances. The Cisco NAC Appliance identifies security issues on laptops and other networked devices, and repairs any vulnerabilities before permitting that device access to the network.

PRODUCT LIST

Security and VPN

- Cisco IPS 4260 Series Sensors
- Cisco Security Agent
- Cisco ASA 5500 and ASA 5540 Series Adaptive Security Appliances
- Cisco Catalyst 6500 Series SPA Line Cards
- Cisco Network Admission Control (NAC) Appliance
- Cisco CS MARS
- Cisco Security Optimization Service

For More Information

For more information, please visit http://www.cisco.com/go/security.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C36-447541-00 01/08

