Maximize WAN Optimization Security and Compliance

Overview
IT decision makers are deploying WAN optimization technology to bring three important business benefits to their organizations:

- Deliver centralized applications with LAN-like speed to remote users, while preserving visibility and branch security.
- Consolidate costly branch office servers, storage and backup infrastructure into data centers, while optimizing WAN bandwidth usage.
- Maximize regulatory compliance and data protection through consolidation of branch storage, as well as acceleration of branch backup applications.

Although WAN optimization solutions accelerates data backup and maintain regulatory compliance over the WAN, most of these solutions pay little attention to protection of data locally stored in branch offices or data in transit over the WAN. This lack introduces security risks because organizations now need to manage two sets of data streams with unequal protection: new, accelerated data flows with little or no protection, and regular flows that are well protected with encryption, stateful firewall protection, and intrusion prevention systems (IPS).

Security administrators struggle to secure data consistently across multiple branch offices worldwide, whether it is data accessed through the LAN or accelerated data sent across the WAN. Many organizations question why they should compromise regulatory compliance certification and face the risks of steep fines to accommodate WAN optimization and whether they can trust WAN optimization over large-scale deployments.

Should optimized data carry higher risks and potentially accelerate the delivery of malicious data across the network? Should organizations face higher risks of not meeting regulatory compliance because of WAN optimization? Should optimized traffic be given equal protection?

This document helps to answer these questions. It describes the security benefits and capabilities offered by Cisco® Wide Area Application Services (WAAS) and discusses several important criteria you should consider before investing in a WAN optimization solution and why these criteria can be important to your business.

Increasing Number of Incidents of Branch-Office Data Leakage
Organizations recently have been faced with increasing numbers of incidents of data leakage. For example, the following incidents made national headlines:

- In March 2006, a file server was stolen from AIG New York containing the personal information of 930,000 customers, including names, Social Security numbers, and tens of thousands of medical records.¹
- On February 25, 2005, Bank of America disclosed that in late December 2004, it lost unencrypted computer backup tapes containing information from 1.2 million federally issued credit cards.²

¹ Source: USA Today (http://www.usatoday.com/money/industries/insurance/2006-06-16-AIG_x.htm).
In June 2005, unencrypted tapes containing information about 3.9 million CitiFinancial branch network customers were lost by United Parcel Service while they were en route to a credit bureau.³

On June 29, 2006, the Nebraska State Treasurer’s Office announced that a hacker broke into a child-support computer system and may have obtained information including the names and Social Security numbers of 300,000 individuals and 9000 employers.⁴

In a survey of 768 IT managers, 81 percent companies reported the loss of one or more laptops containing sensitive information during the past 12 months. Handheld devices and laptops ranked highest among storage devices that posed the greatest risk for sensitive corporate data, followed by universal serial bus (USB) memory sticks, desktop systems, and shared file servers.⁵

In 2006, research by the Ponemon Institute revealed that the average cost of a data breach per record compromised grew 30 percent, averaging a total of $4.8 million per breach.⁶

Forrester Research determined that the cost per breached record ranges from $90 for a low-profile breach in a nonregulated industry to $355 for a high-profile breach in a highly regulated industry.⁷

**Tougher Data Privacy Regulations**

Because of such incidents and the growing concern over data security and risk of leakage, organizations are increasingly being held accountable for complying with a variety of regional, national, international, and industry regulations. The potential penalties for noncompliance include fines, heightened scrutiny, exclusion from programs, credit downgrading, legal prosecution, and imprisonment.

For example, under the Payment Card Industry (PCI) compliance requirements, beginning in October 2006 Level 1 merchants who are out of compliance by storing magnetic strip information from credit cards are subject to significant fines. Card brands are assessing some Level 1 merchants $50,000 to $100,000 per month. Sarbanes-Oxley has resulted in individual fines of over $20 million for chief executive officers (CEOs), such as the GemStar CEO who was fined $22 million in May 2006.

Table 1 shows some of the compliance regulations that businesses and governments must follow today.

**Table 1. Data Privacy Compliance Regulations**

<table>
<thead>
<tr>
<th>Regulation</th>
<th>Information Protected</th>
<th>Date of Enforcement</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIPAA</td>
<td>Health information of patients</td>
<td>1996</td>
</tr>
<tr>
<td>GLBA</td>
<td>Consumer Financial Information</td>
<td>1999</td>
</tr>
<tr>
<td>SOX</td>
<td>Business Financial and Accounting Information</td>
<td>2002</td>
</tr>
<tr>
<td>CA SB 1386*</td>
<td>Consumer Personal Information</td>
<td>2003</td>
</tr>
<tr>
<td>PCI</td>
<td>Credit Card Information</td>
<td>2005</td>
</tr>
</tbody>
</table>

* Security Breach Laws in More than 34 States.

² Source: Associate Press and MSNBC (http://www.msnbc.msn.com/id/7032779/).
⁴ Source: Associated Press.
⁵ Source: Ponemon Institute and Vontu.
Organizations Are Responding

Three surveys across multiple industries, conducted by Infonetics, Taneja Group, and Ponemon Institute and Vontu, indicated a clear and consistent trend: Data encryption and protection must be built into WAN optimization technologies.

- Integrated security: According to Infonetics, the top emerging technology trend, regardless of site type or timeframe, is the integration of security features such as firewalls, VPNs, and intrusion detection systems (IDSs) into routers. This trend is validated by the recent rapid adoption of integrated security embedded in Cisco Integrated Services Routers. Organizations have been implementing integrated firewall and IDS and IPS security at the branch office, in addition to link-level security such as Multiprotocol Label Switching (MPLS) links. Organizations are using these integrated security features to protect against split VPN use and prevent viruses from propagating in the branch network (Figure 1).

Figure 1. Mainstream Adoption of Integrated Security

- Secure optimization: According to the Taneja Group survey, 250 IT directors require optimization to preserve their integrated security investment. Their top priority for a remote-office and back-office (ROBO) solution is security, with network optimization next, as shown in Figure 2.
• Management, optimization, and protection: According to the same Taneja Group survey, 250 IT directors sum up their top three challenges for ROBO environments as management, WAN optimization, and data protection for locally stored data (Figure 3).

Figure 3. Top Challenges in Remote-Office Deployments

• Encryption: The Taneja Group survey also indicated that IT directors consider data encryption to be essential (Figure 4).
Figure 4. Security Element Deployment at ROBO Sites

Security Elements Deployment at ROBO Sites

- Protection of data at rest: In the Ponemon Institute and Vontu survey, 81 percent of the 500 IT directors indicated that protecting sensitive data at rest is a priority this year, and 89 percent predicted that it will be a priority next year. Spending priorities will increasingly focus on e-mail, file servers, mobile devices, and backup (Figure 5).

Figure 5. Protecting Data at Rest

Cisco Secure WAN Optimization Solution and Benefits

In addition to the expected benefits of application acceleration and branch-office IT infrastructure consolidation, Cisco WAAS incorporates security and data protection capabilities to help ensure consistent security across both accelerated and regular flows (Figure 6).
**Figure 6. Data Protection Capabilities of Cisco WAAS Solution**

- **Disk encryption**: Encryption of all optimization data on the remote Cisco Wide Area Application Engine (WAE) Appliance or network module prevents unauthorized data access or theft. Federal Information Processing Standard (FIPS) 197 approved technologies and Advanced Encryption Standard (AES) 256-bit encryption are used to encrypt data on the Cisco WAE disk drives. The automated centralized key management service, integrated within the Cisco WAAS Central Manager, simplifies management of encryption keys, provides centralized failover capability for high availability, and supports backup and restoration of keys to offline vaults for disaster recovery purposes.

- **Regulatory compliance**: Cisco WAAS is designed and rigorously tested for compliance with major industry security standards. Cisco WAAS is the only WAN optimization solution to be listed in the Common Criteria Evaluation and Validation Scheme (CCEVS), also known as ISO 15408. The CCEVS is the leading program of the National Information Assurance Partnership (NIAP), a U.S. government initiative of the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) designed to increase the level of consumer trust in information systems and networks. Furthermore, Cisco WAAS maintains compliance with stateful firewall operation, which is required in compliance standards such as the PCI standard.

- **Stateful firewall protection**: Cisco is the only vendor that supports stateful inspection of WAN-optimized traffic through certified interoperability between Cisco firewalls and Cisco WAAS. For the first time, organizations can receive equal protection for optimized traffic and regular traffic without compromise.
  - Full compliance with firewall policies and access control lists (ACLs) through packet header transparency
  - Full compliance with stateful firewall protection for individual, end-to-end traffic that is optimized
  - With Cisco WAAS, no need for additional ports to be opened on the firewall except for those for management and CIFS acceleration

- **IPS interoperability**: Cisco IPS provides virus scanning in the network and prevents the propagation of other malicious data while maintaining full interoperability with Cisco WAAS.
This feature allows customers to perform WAN optimization while protecting their networks against viruses.

- **Role-based access control (RBAC):** The Cisco WAAS Central Manager offers authentication, authorization, and accounting (AAA) integration with external authentication providers such as Microsoft Active Directory, RADIUS, and TACACS+. Cisco WAAS is the only leading WAN optimization product that provides flexible RBAC for deployment. Customers can create profiles based on role, department, responsibility, and other parameters to help ensure secure access to only the portions of the system that are required. Role-based access is a requirement in many compliance regulations.

**Conclusion**

Protecting branch-office data is increasingly difficult as a result of globalization, decentralized operations, and rising risks of data leakage. At the same time, the number of compliance regulations is increasing. Traditional WAN optimization solutions offer neither strong disk encryption to protect data at rest nor integration with security infrastructure to provide protection for optimized data in transit. Organizations need equal data protection for both accelerated and regular data.

Cisco offers a complete, secure WAN optimization solution, with ISO 15408 certification, compliance regulation support through strong disk encryption, stateful firewall, IPS integration, and RBAC, and equal stateful protection of accelerated and regular data. When used together, Cisco routers, firewalls, and IPS, along with Cisco WAAS, maximize security while optimizing the WAN, thus enabling organizations to confidently deploy large-scale WAN optimization, reduce branch-office IT costs, and improve user productivity.

**For More Information**


Use the selection criteria shown in Table 2 to compare Cisco WAAS security capabilities to those of other WAN optimization products.

**Table 2.** Cisco WAAS Security Capabilities

<table>
<thead>
<tr>
<th>Benefits</th>
<th>Cisco WAAS</th>
<th>No Optimization</th>
<th>Other Optimization Products</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stateful Firewall Protection</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Stateful Protection of Accelerated Data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No Additional Static Ports Open</td>
<td>✔</td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Compliant with Cisco IOS Firewall</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliant with Cisco PIX Firewall</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliant with Cisco Firewall Switching Module</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliant with Cisco Adaptive Security Appliances</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regulatory Compliance</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maintain PCI 1.1 Compliance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Common Criteria EAL4 Evaluation Accepted</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interoperable with Intrusion Prevention Systems (IPS)</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inline Virus Scanning</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Out of Path Virus Scanning</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Disk Encryption
- 256-bit AES with FIPS Level 2 Specs

## Centralized Key Management
- with Failover and High Availability

## No Key Left on Disks

## Centralized Key Backup and Restoration

## Role-based Access Control
- Microsoft Active Directory

## RADIUS

## TACAS+

### Note:*
For firewalls other than Cisco IOS Firewall, static ports need to be open only for CIFS and management.