IBM Managed Network Security Services for AWS

Your network security partner with global reach

Managing network security devices can help organizations prevent various threats. However, the costs and complexity associated with traditional device management solutions may be high. Resources or expertise are required to take care of the finer details like designing and deploying the right security policy.

For organizations that need to reduce the cost and complexity of managing network and endpoint technology on AWS, IBM Security Services helps to optimize the value of existing security investments while delivering near-continuous management and analysis.

IBM Security Services provides management, monitoring, and alerting of security devices in the cloud or on the customer premises:

- Network Intrusion Detection/Prevention System (NIDS/NIPS)
- Firewalls and Policy Management
- AWS-native Firewalls, Network Access Control List (NACL) and security groups support
- Distributed Denial of Service (DDoS) Mitigation
- Web Application Firewall (WAF)

Highlights

- IBM's Managed Network Security Services options for AWS
- Key drivers of managed network security
- Types of network security services offerings

IBM Security Services supports a matrix of thoroughly tested and industry leading vendor platforms and technologies including Check Point, Fortinet, Juniper, Palo Alto, SOPHOS and Cisco devices, and virtual software installed in your environment, or in AWS, Azure, and IBM cloud. Services are delivered from a network of global IBM Security Operations Centers (SOCs).

Key Drivers for Managed Network Security

- Preemptive protection from known and emerging security threats
- Support and simplify adoption of AWS network controls
- Multivendor support that helps maximize existing security investments
- Real-time views of security posture to reduce risk and improve regulatory compliance
- Resolution of security issues in expedient and cost-effective processes
- Guaranteed service levels designed to ensure business continuity
- Comprehensive audit reports including executive and technical reporting options
- Potential for lower total cost of ownership due to reduced staffing requirement and reduced maintenance, infrastructure and training costs
- Customizable service options to fit specific business requirement

Network Intrusion Detection/Prevention System (NIDS/NIPS)

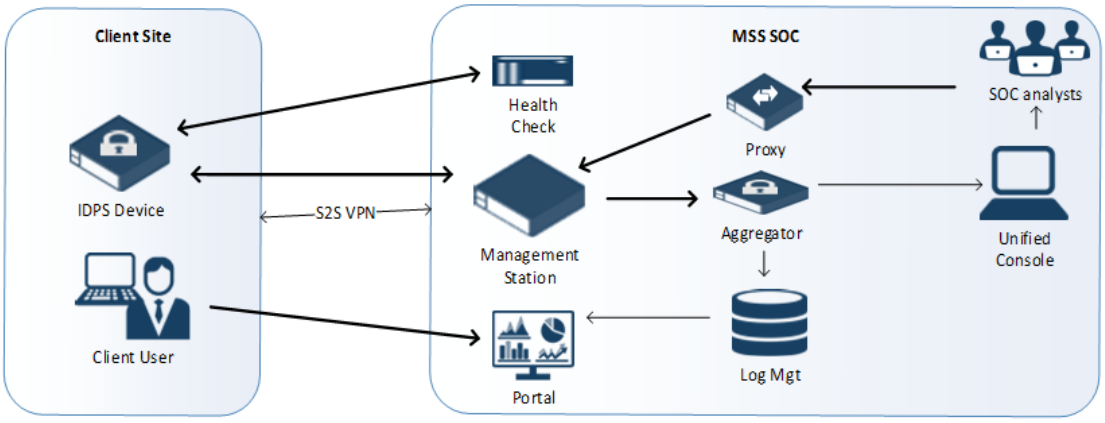
Intrusion Detection reports on violations against security policies. Intrusion Prevention implements protections against those violations.

Most solutions add the protection as an option; hence these devices are usually called Intrusion Detection/Prevention Systems or IDPS.

IBM-managed Intrusion Detection and Prevention System (IDPS) can provide clients vital visibility into security events and is designed to provide active protection for networks to avoid costly downtime or breaches. In addition to having events monitored, IBM can also maintain and manage the IDPS devices and policies, receive event logs, and monitor system health and uptime.

Key features provided with the managed IDPS services include the following:

- Automated event correlation and alerting
- IBM® X-Force® Threat Analysis Service (security intelligence): Subscription to this additional service provides more proactive network protection
- Device monitoring and management
- Health checks
- Policy tuning



Managed Network Security Services for Intrusion Detection and Prevention Systems

Firewalls and Policy Management

A network-based firewall provides our clients with a first line of defense in a multi-layered in-depth protection strategy. By utilizing stateful packet inspection and customized security policies, the firewall prevents unwanted traffic from entering or leaving the enforcement point. Granular control over ingress/egress traffic can protect potentially vulnerable services, applications or data from exploit, and contributes to compliance for end user acceptable use policies.

IBM Firewall Management Services provides monitoring and security policy management of traditional and next-generation network firewalls. Key features provided with the managed firewall services include the following:

- Centralized device management and policy enforcement
- Health monitoring
- Malware defense
- Log correlation and retention
- Robust portal for client visibility of security status and interactions
- Detailed reporting for improved decision making

Firewall Policy Management Automation

Utilizing Artificial Intelligence, IBM Security Services can automatically receive, approve, review, implement and validate policy change requests. This historically manual process is automated and requires minimal human touch (eliminating human error and adding the speed of automation) to manage clients' security policies.

AWS-native Firewalls, Network Access Control List (NACL) and security groups support

This service is explicitly built to support the native network security features of AWS such as AWS Network Firewall, NACLs and Amazon Elastic Compute Cloud (EC2) security groups.

Services include:

- Management, monitoring, alerting, governance and reporting of native cloud security controls & policies
- Manage: Manage and troubleshoot security controls and policies for ongoing protection of the AWS environment
- Governance: Gain confidence in the security maturity through relevant reporting, insights, and recommendations

Distributed Denial of Service (DDoS) Mitigation

This service is explicitly built to steady state support for the native network security features of AWS Shield Advanced and other ISV partners like Fortinet, Check Point, Cisco, Barracuda, and SOPHOS.

- DDoS policy management, blocking malicious web traffic / DDoS flooding in response to a Priority Level 1 or 2 Incident
- Investigate performance issues and generate monthly web traffic management reports. The service will allowlist / blocklist IP addresses working closely with the network teams for each of the websites (Geo tagging allow / block)
- Deploy redirect rules on specific websites as and when required

Managed Web Application Firewall (WAF)

This service is explicitly built to steady state support for the native network security features of AWS WAF and other WAF ISV partners like Palo Alto and Zscaler.

- Steady state support for AWS WAF and Security Competency ISV partners with standard 8x5 support provided and severe business interruption (Severity 1) technician available 24/7 (On-Call).
- IBM Security can also customize support hours based on client requirement, like 24/7,16/5, 24/5-365 days support
- On-boarding or off-boarding of externally facing web applications into AWS WAF or ISV WAF
- Health checks to ensure the WAF gateway systems are functioning as designed, WAF policies are managed, and web traffic is blocked in response to a Priority Level 1 or 2 Incident
- Investigation of WAF performance issues and generate monthly Web traffic management reports

Why IBM?

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, provides security solutions to help organizations drive security into the fabric of their business so they can thrive in the face of uncertainty.

IBM operates one of the broadest and deepest security research, development and delivery organizations. Monitoring more than one trillion events per month in more than 130 countries, IBM holds over 3,000 security patents. To learn more, visit ibm.com/security.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice and represent goals and objectives only.

For more information

To learn more about IBM Offering Name, please contact your IBM representative or IBM Business Partner, or visit the following website https://www.ibm.com/security/services/managed-security-services