IBM Managed Network Security Services

Your network security partner with global reach and localized delivery

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 policies.

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

IBM® Managed Network Security Services provides management, monitoring and alerting of security devices in the cloud or on your premises:

- Firewalls and Policy Management
- Virtual Private Network Support
- Unified Threat Management (UTM)
- Intrusion Detection and Prevention Systems (IDPS)
- Secure Web Gateways (SWGs)
- Secure Web Access (SWA)

Managed Network Security Services supports a matrix of thoroughly tested and industry leading vendor platforms and technologies including CheckPoint, Fortinet, Juniper, Palo Alto 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) operating 24 hours a day and 365 days a year.

Highlights

- The case for managed network security
- Key drivers of managed network security
- Types of network security services offerings

IBM

Key Drivers for Managed Network Security

- Preemptive protection from known and emerging security threats
- Multivendor support that helps maximize existing security investments
- Near 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, maintenance, infrastructure and training costs
- Customizable service options to fit specific business requirements

Firewall and Policy Management

A network-based firewall provides you 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 Security provides monitoring and security policy management of traditional and next-generation network firewalls. Key features provided with the managed firewall services include:

- Centralized device management and policy enforcement
- Health monitoring

- – Malware defense
- – Log correlation and retention
- – Robust portal for visibility of security status and interactions
- – Detailed reporting for improved decision making

Firewall Policy Management Automation

Utilizing artificial intelligence (AI), 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 your security policies.

Virtual Private Network Support

IBM enables client-requested VPN features of the firewall and UTM agent as Site-to-site VPNs, Client-to-site VPNs, Secure Sockets Layer (SSL) VPNs.

Unified Threat Management

Managed Unified Threat Management (UTM) services from IBM Security can help protect your business with premium monitoring and support of UTM devices or agents are provided with a base Protection Package (IPS and firewalls) and an optional Content Package add-on (web filtering, SSL enforcement, anti-spam/anti-virus modules).
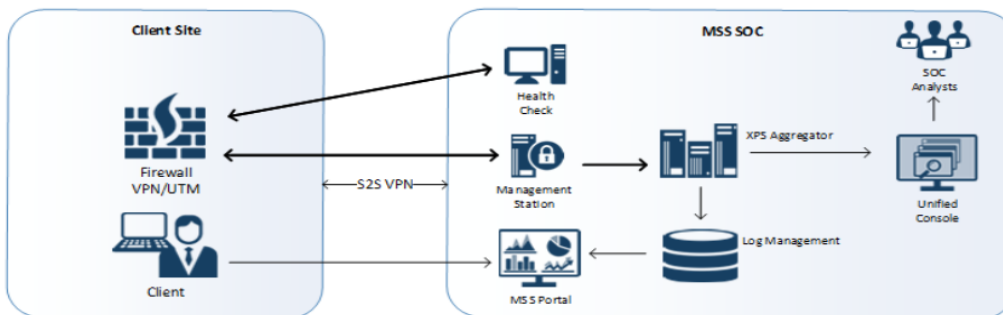
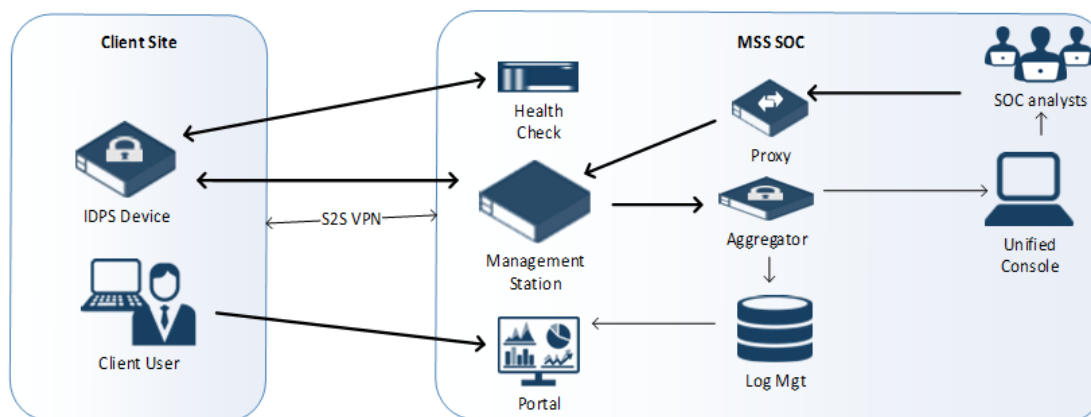*Managed Network Security Services architecture for next-generation firewall/UTM and VPN*

Intrusion Detection and Prevention System

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 IDPS can provide you vital visibility into security events and is designed to deliver 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:

– Automated event correlation and alerting
– IBM Security X-Force® Threat 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

Secure Web Gateways

IBM MSS provides near real-time threat analysis and forensic reporting solutions for secure web gateways that you may need to defend against advanced attacks.

Key features provided with the managed SWG services include:

- Security monitoring and management
- Robust portal for visibility of security status and interactions
- Centralized device management and policy enforcement
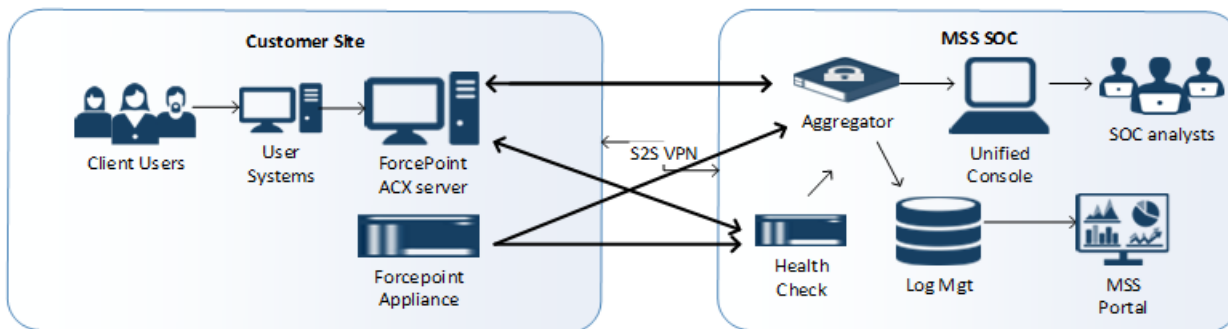
Managed Network Security Services – Secure Web Gateway

Secure Web Access

Secure Web Access (SWA) addresses the need to secure internet browsing of your employees and users by filtering website categories, protecting against malware and viruses, and providing authentication and reporting of the web access. Additionally, these solutions offer a hybrid cloud functionality for remote user access.

Key features provided with the managed SWA services include:

- User authentication
- Web and URL filtering
- Data loss prevention
- SSL inspection, and visibility of encrypted traffic
- Ability to stream decrypted content to an external server
- Content caching
- Bandwidth management
- Stream-splitting
- Social media controls
- Manage use of Facebook, LinkedIn and other social media websites through highly granular rules
- Data capture
- Import security incidents and forensic details into Security Information and Event Management (SIEM) solutions
- Robust reporting
- Includes more than 60 pre-defined, easily customizable report widgets
- Advanced threat dashboard
- Provides actionable forensic detail on who was attacked, what data was attacked, where the data almost went and how the attack was executed

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 Security 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.

![IBM logo]

For more information

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