Managed UTM Service
(Unified Threat Management)

Mit Managed UTM schützen Sie Ihr Unternehmen optimal vor Gefahren aus dem Internet. Damit kann der Sicherheitslevel von einer traditionellen Firewall auf einen multifunktionalen Schutz erhöht werden.

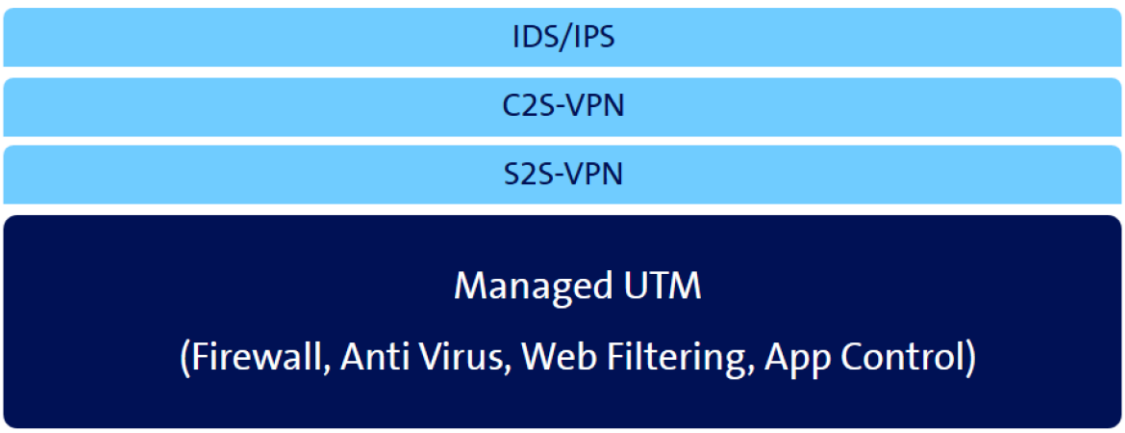
Stateful Inspection
Umfasst Spoofing und Packet Filtering. Spoofing sind Methoden, mit denen sich Authentifizierungs-und Identifikationsverfahren untergraben lassen – sofern sie auf der Verwendung vertrauenswürdiger Adressen oder Hostnamen in Netzwerkprotokollen beruhen. Packet Filtering ist eine dynamische Filtertechnik, die jedes Datenpaket einer Session zuordnet. Die Pakete werden analysiert und in dynamischen Zustandstabellen gespeichert. Pakete, die nicht vordefinierten Kontakten zugeordnet werden können oder allenfalls zu einer DoS-Attacke gehören, werden verworfen.

Zonenbasierte Policy
Zusätzlich zu Source und Destination Adresse wird die Angabe einer Source und einer Destination-Zone verlangt. Befindet sich eine Source nicht in der zugeordneten Zone, wird das Paket von der Firewall verworfen..

Anti-Virus
Via Policy wird entschieden, welche Protokolle auf Viren, Malware und weitere Schadsoftware untersucht werden. Swisscom verwendet eine Standard Policy, welche nach Best Practice arbeitet. Die regelmässige Aktualisierung der Signaturdatenbank erfolgt automatisch und wird überwacht.

Web-Filtering
Alle bekannten Webseiten des Internets werden durch den Hersteller in Kategorien eingeteilt. Mittels Standard Policy blockiert Swisscom den Zugriff auf spezifische Kategorien. Es gibt die Möglichkeit, einzelne gesperrte URL in den Kategorien freizuschalten. Swisscom verwendet die vom Hersteller angebotenen Kategorien und Unterkategorien des Service.

Application Control
Mit der Funktion Application Control kann der Zugriff auf Applikation erlaubt oder blockiert werden. Swisscom blockiert vordefinierte Applikationskategorien. Auf Wunsch des Kunden können weitere Kategorien gesperrt oder einzelne Applikationen erlaubt werden.



Optionale Zusatzleistungen

VPN (Site-to-Site)
Mit dem Protokoll IPSec sorgen wir für eine sichere Verbindung zwischen zwei Standorten. Voraussetzung ist, dass die Standorte mit einem Netzwerk (Internet, MPLS, etc.) verbunden sind. In den meisten Fällen wird dazu das Transportmedium Internet verwendet. Diese Verbindung kann mit einer Partner Firewall erstellt werden oder mit dem Managed VPN Service der Swisscom.

VPN (Client-to-Site)
Um einen sicheren Firmenzugang Ihrer End-User zu ermöglichen, wird eine Client-to-Site Lösung basierend auf dem Protokoll SSL offeriert. Sicherheitseinstellungen werden auf dem Gateway pro Profil definiert.
Die einfache Benutzer Authentisierung (User/PW) kann mittels Anbindung an Ihren Directory Server (ADS, Radius, etc.) sichergestellt werden.

IDS/IPS
Zum Schutz des Firmennetzwerkes wird die Kommunikation mit einem Best Practice Signaturset der Swisscom abgesichert. Dieses beinhaltet Signaturen zum Schutz von eingehendem und ausgehendem Datenverkehr.

Hybrid UTM (Cloud-based)
Performance-intensive Leistungen wie URL-Filtering, Anti-Virus, Sandboxing etc. werden in der Swisscom Cloud erbracht. Die Swisscom Cloud befindet sich in Schweizer Data Centers und wird aus der Schweiz betrieben. Dadurch können die Systeme vor Ort (premise based) entlastet werden und skalieren auch bei schneller Zunahme von Userzahlen und weltweiter Verteilung.

Wiederkehrende Leistungen

Health Incident Monitoring und Management	Swisscom garantiert, dass Health Incidents innerhalb der definierten Service-Level-Zeiten bearbeitet werden. Kann ein Security Device nicht erreicht werden, übernimmt Swisscom die Fehlerbehebung und informiert Sie umgehend.
Security Incident Monitoring und Management	Aus den Log Daten der Firewall werden Events erstellt, welche mit der Threat Intelligence auf Bedrohungen analysiert werden. Bei einem Verdacht wird ein Security Incident erstellt, welcher in unterschiedliche Klassen (Insufficient Info, Harmful Attack, Harmless Attack, False Positive) eingeteilt wird. Die Klassen Insufficient Info und Harmful Attack werden von einem Spezialisten analysiert und gezielt an Sie eskaliert.
Change-Management	Sie bewerten die Dringlichkeit der Umsetzung eines Change. Swisscom unterscheidet zwischen Minor- und Major-Change. Minor Change sind Servicebestandteil. Diese werden direkt im MSS-i-Dashboard in Auftrag gegeben.
Release Management	Swisscom testet Hersteller Releases der Managed Devices nach definiertem Testkatalog im Labor und implementiert diese nach der Freigabe. Beim VPN Client werden ausschliesslich Basis Connectivity Tests am Gateway gemacht.
Vulnerability Management	Bei Veröffentlichung einer kritischen Schwachstelle eines Managed Devices übernimmt Swisscom eine proaktive Rolle und informiert Sie und stellt die Eliminierung der Schachstelle nach Best Practice sicher.
Signatur und Kategorie Management Proxy-, Web-Antivirus- und Web-Filter-Management	Bestandteil vom Service ist die automatische Aktualisierung von Hersteller Updates wie Signaturen, Kategorien und neuen Applikationen. Signaturen werden täglich an Randzeiten auf dem System eingespielt. Änderungen der Kategorien oder Applikationen werden in regelmässigen Abständen durchgeführt. Sämtlich Changes werden nach Best Practice ohne Change Request durchgeführt.
Configuration und Backup Management	Swisscom kümmert sich um alle aktuellen Konfigurationen und stellt sicher, dass Backups sicher und nachvollziehbar gelagert werden. Dadurch können ältere Konfigurationen bei Bedarf wieder zurückgespielt werden.
Life Cycle Management	Swisscom verwendet ausschliesslich Hard- und Software, die dem aktuellen Stand der Technik entspricht.
Reporting	Ausführliche Reports können Sie via MSS-i-Dashboard individuell zusammenstellen. Entsprechend dem Service Level werden Verfügbarkeit, Ticketstatus (Incident- und Change-Management) sowie Management Reports automatisch erstellt.

Supportzeit 5x11	○
Security Dashboard	●
Service Level	Standard, Premium, Platinum
Data Retention: Logdaten und Requests: 1 Jahr	●
Data Retention: Backup 30 Tage	●

● = Standard ○ = Option wählbar ⊙ = gegen Aufpreis

Technische Features	
Release Management inkl. Testing	●
Vulnerability Management	●
Automatisierte Log Analyse auf Security Incidents (SLA Premium, Platinum)	●
On Premise Device	●
Virtual Device	○
Read-Only Access	⊙
Logdaten an Syslogserver senden	⊙
Site-to-Site VPN	⊙
Client-to-Site VPN	⊙
Intrusion Detection System (IDS/IPS)	⊙

● = Standard ○ = Option wählbar ⊙ = gegen Aufpreis

Swisscom, der richtige Partner

Swisscom unterhält die Schweizer Einsatzzentrale für Netzwerksicherheit. Mit 24h-Betreuung durch ausgewiesene Spezialisten, jederzeit aktuellen Zertifizierungen und für die Schweiz optimierter Threat Intelligence. Die sichere Lösung für Schweizer Unternehmen.

Weitere Informationen zum Service: www.swisscom.com/mss-i

Das ist Ihr Nutzen

> Sie wissen, dass Ihre Systeme stets auf dem neusten Stand ist
> Sie können den Service jederzeit in Ihre Infrastruktur integrieren und modular erweitern
> Sie sind dank dem MSS-i Dashboard laufend über den Status Ihrer Services informiert
> Sie profitieren von 7 x 24 h Monitoring in Echtzeit durch ausgewiesene Sicherheitsexperten