Managed Firewall Service

Damit bei Ihnen nicht jeder ein- und ausgeht, wie er will.

Schützen Sie Ihr Firmennetz zuverlässig vor Angriffen aus dem Internet. Mit dem Managed Firewall Service profitieren Sie neben dem grundlegenden Porthandling von weiteren Funktionen.

Folgende Leistungen sind integraler Servicebestandteil:

Network Adress Translation (NAT)
Ändert auf der Firewall die IP-Adressinformationen der Pakete. Dadurch ist die Firewall während einer Session die einzige Instanz, die alle Adressierungsinformationen enthält.

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.

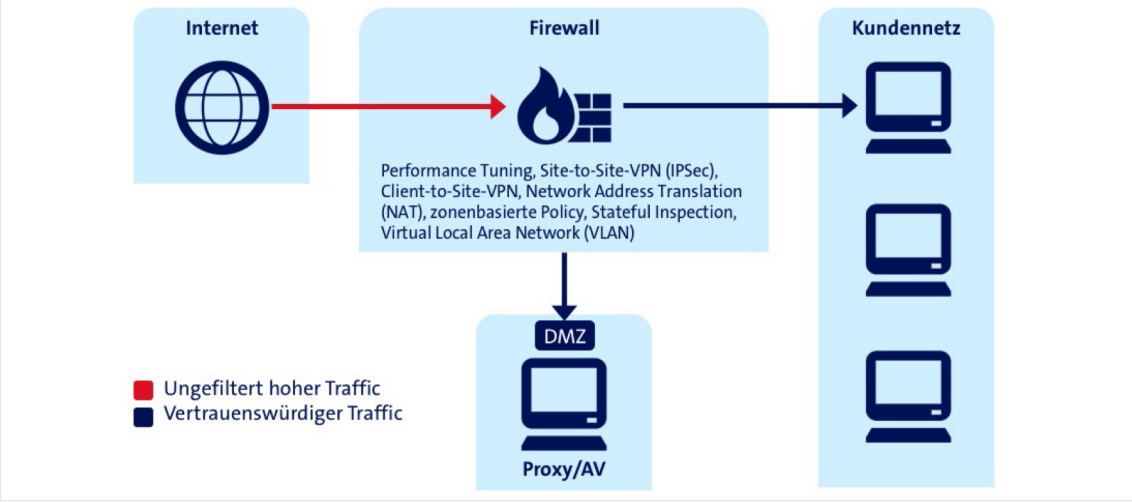
Zonenbasierte Policy
Source und die Destination-Adresse werden geprüft. Zusätzlich wird die Angabe einer Source und einer Destination-Zone verlangt. Befindet sich eine Source nicht in der zugeordneten Zone, wird das Paket von der Firewall verworfen.

Performance Tuning
Erreichen der maximale Leistung der Systeme. Dazu sind eine optimale und aktuelle Policy sowie spezifische Einstellungen auf der Firewall notwendig.

Virtual Local Area Network (VLAN)
Logisches Teilnetz innerhalb eines physischen Netzwerkes. Datenpakete von Firewall, Router und Switches werden in Teilnetze weitergeleitet.

Clustering
Bei entsprechendem Service-Level-Agreement wird ein Cluster bestehend aus zwei Managed Devices installiert. Der Cluster kann an einem oder verteilt auf mehrere Standorte aufgebaut werden. Der Betrieb wird in einem Activ/Passiv Modell erbracht.

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.



Optionale Zusatzleistungen

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.

VPN (Client-to-Portal)
Mittels Web Portal können Sie Ihrem Partner sicheren Zugriff für einer Vielzahl Ihrer Unternehmens-Applikationen gewähren. Dem Partner müssen Sie keine Endgeräte zur Verfügung stellen.

Starke Authentisierung
Erhöhung der Zugriffssicherheit durch eine Zwei- Faktor-Authentisierung mit Benutzername und Passwort sowie Mobile ID oder One-Time-Token (SMS, SW- und HW-Token) als zweiten Faktor. Die Benutzerverwaltung und das Reporting erfolgt via eService-Portal.

Quality of Service
Das Daten-Paket kommt mit einem DSCP Wert bei der Firewall an. Die Firewall priorisiert dieses Daten-Paket entsprechend dem DSCP Wert. Der DSCP Wert wird dabei nicht verändert. Voraussetzung für diese Option ist ein ganzheitliches QoS Konzept des Kunden, in dem die Firewall integriert wird.

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 Changes. Swisscom unterscheidet zwischen Minor- und Majo-Changes. Minor Changes 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.
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.

Service Optionen	
Supportzeiten 7x24	●
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	●
Individuelle Policy	○
On Premise Device	●
Virtual Device	○
Read-Only Access	⊙
Logdaten an Syslogserver senden	⊙
Client-to-Site VPN	⊙
Client-to-Portal VPN	⊙
Authentication (LDAP, Radius, Zertifikate, Strong Authentication)	⊙
Intrusion Detection System (IDS)	⊙

● = 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 Firewall stets auf dem neusten Stand ist
- Die Firewall Log Daten werden mittels Threat Intelligence analysiert
- Sie können den Service jederzeit in Ihre Infrastruktur integrieren und modular erweitern
- Der Schutz von virtuellen Server innerhalb von Dynamic Computing Service kann von MSS-i angeboten werden.
- Sie sind dank dem MSS-i Dashboard laufend über den Status Ihres Services informiert
- Sie profitieren von 7 x 24 h Monitoring in Echtzeit durch ausgewiesene Sicherheitsexperten