WHITE PAPER

Schützen des Netzwerks von innen

Internal Segmentation Firewall (ISFW)

Zusammenfassung

Inhaltsverzeichnis

Seit zehn Jahren versuchen Unternehmen, ihre Netzwerke durch Abwehrmaßnahmen an deren Außengrenzen zu schützen. Dazu gehören die Schnittstelle zum Internet, der Perimeter, Endgeräte und Rechenzentrum (einschließlich DMZ). Dieser Ansatz des Schutzes „von außen nach innen“ beruht seit jeher auf der Vorstellung, dass Unternehmen klar definierte Zugänge überwachen und ihre wertvollen Ressourcen sichern können. Die Strategie bestand darin, einen möglichst unüberwindlichen Verteidigungswall an der Grenze aufzubauen (Firewall) und davon auszugehen, dass dieser nicht zu überwinden ist.

Aber Unternehmen wachsen und führen neueste Technologien wie Mobilität und Cloud ein und machen dadurch die Kontrolle und Sicherung der herkömmlichen Netzwerkgrenzen zunehmend komplexer. Inzwischen gibt es viele verschiedene Möglichkeiten, in ein Unternehmensnetzwerk einzudringen.

Vor nicht allzu langer Zeit kennzeichneten Anbieter von Firewalls die Ports ihrer Geräte noch mit „Extern“ (nicht vertrauenswürdig) und „Intern“ (vertrauenswürdig). Komplexe Bedrohungen nutzen dies jedoch zu ihrem Vorteil, denn sind die Grenzen des Netzwerks einmal überwunden, ist dieses sehr flach und offen. Die Geräte im Inneren des Netzwerks sind meist kaum geschützt wie Switches, Router und sogar Bridges. Wenn ein Hacker, ein bezahlter Angreifer oder gar ein verprellter Mitarbeiter erst einmal Zugriff zum Netzwerk erlangt hat, steht ihm das gesamte Unternehmensnetzwerk mit all den wertvollen Ressourcen offen.

Die Lösung ist eine neue Art von Firewall – die Internal Segmentation Firewall (ISFW) – die strategische Punkten des internen Netzwerks überwacht. Sie kann bestimmten Servern vorgeschaltet sein, auf denen wertvolles geistiges Eigentum gespeichert ist, oder einer Reihe von Endnutzergeräten oder Webanwendungen in der Cloud überwachen.

Wichtige Anforderungen

- **UMFASSENDER SCHUTZ**: Kontinuierlicher Schutz von innen vor komplexen Bedrohungen mit einer einzigen Sicherheitsinfrastruktur
- **RICHTLINIENBASIERT:** Zur besseren Kontrolle und Segmentierung von Benutzern und zur Beschränkung der Zugangs zu sensiblen Ressourcen für Bedrohungsvektoren
- **EINFACHE IMPLEMENTIERUNG**: Der Standard-Transparent-Modus macht eine Umgestaltung der Netzwerkarchitektur überflüssig und wird zentral implementiert und verwaltet.
- **HOHE LEISTUNG**: Leistung von mehreren Gigabit unterstützt „East-West-Traffic“ in Leitungsgeschwindigkeit

Sobald die ISFW eingerichtet ist, muss sie den ein- und ausgehenden Datenverkehr dieser spezifischen Netzwerkressource unmittelbar „sichtbar“ machen. Diese Sichtbarkeit wird sofort gebraucht, ohne monatelange Netzwerkplanung und -implementierung.

Vor allem muss die ISFW auch „Schutz“ bieten, denn Erkennung ist nur ein Teil der Lösung. Das Durchsuchen von Protokollen und Warnmeldungen kann Wochen oder Monate in Anspruch nehmen. Die ISFW muss eine proaktive Segmentierung bieten und Echtzeitschutz, der auf den neuesten Sicherheitsupdates basiert.

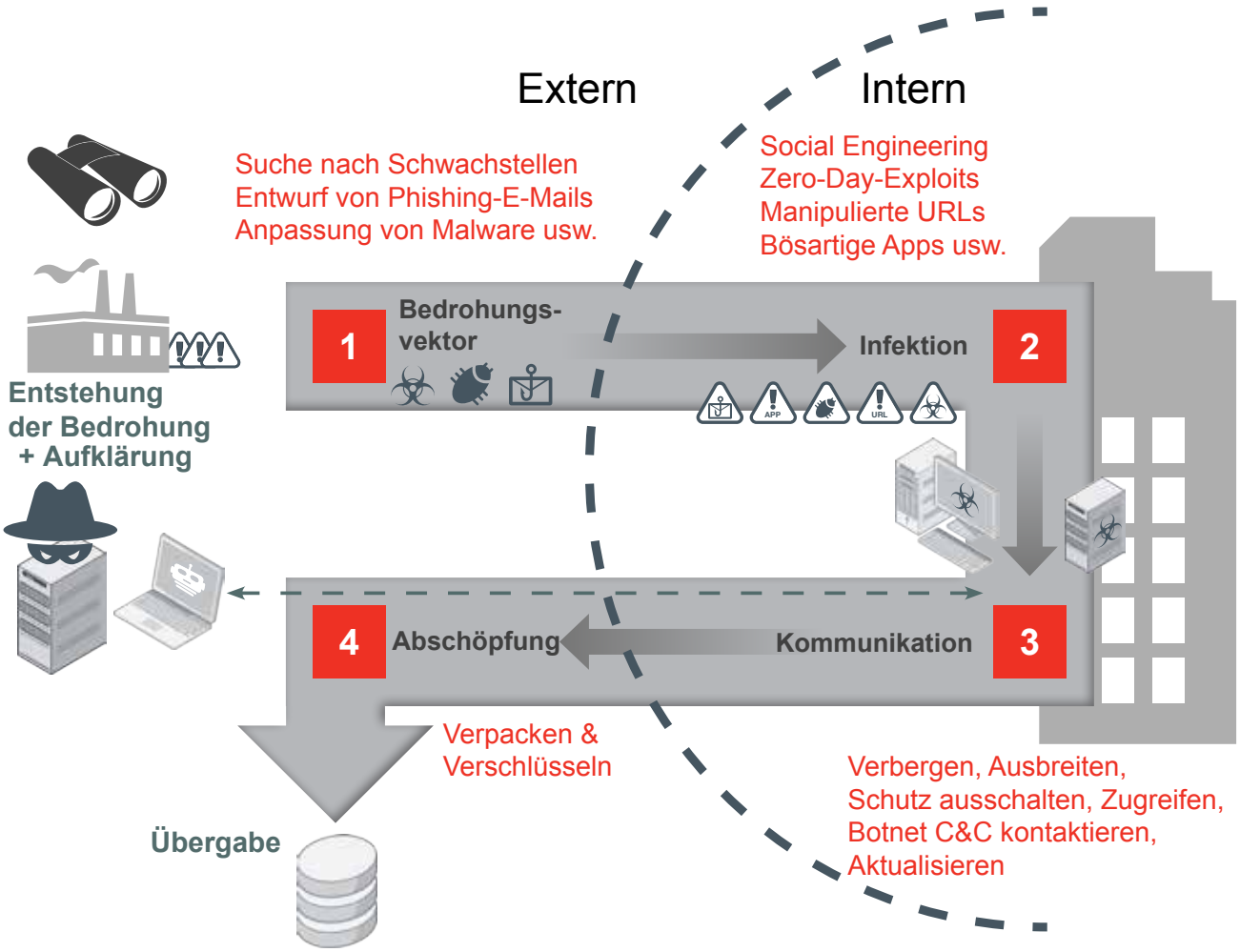
Schließlich muss die ISFW so flexibel sein, dass sie an jeder Stelle im internen Netzwerk platziert und in andere Teile der Sicherheitslösung des Unternehmens integriert und gemeinsam verwaltet werden kann. Weitere Sicherheitslösungen können noch zusätzliche Sichtbarkeit und zusätzlichen Schutz bieten. Dazu gehören E-Mail-Gateway, Web-Gateway, äußere Firewalls, Cloud-Firewalls und Endgeräte. Zudem müssen Internal Segmentation Firewalls an verschiedenste Datendurchsätze (von gering bis hoch) anpassbar sein und im gesamten Netzwerk implementiert werden können.

Komplexe Bedrohungen nutzen das „flache interne“ Netzwerk aus

Cyberkriminelle entwickeln individuelle Angriffe, um die herkömmlichen Verteidigungsmechanismen auszuhebeln und nach ihrem Eindringen eine Erkennung zu verhindern und das Abschöpfen wertvoller Daten zu ermöglichen. Sind die Netzwerkgrenzen erst einmal überwunden, gibt es nur noch wenige Systeme, die komplexe persistente Bedrohungen (APT) erkennen oder davor schützen können.

Der Bedrohungszyklus in Abbildung 1 zeigt, dass nach dem Überwinden der Perimetergrenze die Aktivitäten mehrheitlich innerhalb der Netzwerkgrenze stattfinden. Im Rahmen dieser Aktivitäten werden beispielsweise agentenbasierte Sicherheitsmaßnahmen deaktiviert, Updates über das Botnet-Befehls- und Steuerungssystem durchgeführt und die anvisierten Ressourcen werden zusätzlich infiziert/instrumentalisiert und extrahiert.

ABBILDUNG 1 – LEBENSZYKLUS KOMPLEXER BEDROHUNGEN



Die Antwort ist eine neue Art von Firewall – die Internal Segmentation Firewall (ISFW)

Die Entwicklung von Firewalls konzentrierte sich in den vergangenen zehn Jahren meist auf die Netzwerkgrenze, die Schnittstelle zum Internet, den Perimeter (Host-Firewall), Endgeräte, das Rechenzentrum (DMZ) oder die Cloud. Den Anfang machte die zustandsabhängige Firewall. Eine Weiterentwicklung stellte das Unified Threat Management (UTM) für dezentrale Netzwerke dar, das Firewall, Angriffserkennung und Antivirus vereinte. Später kam die Next Generation Firewall (NGFW), die noch Intrusion Prevention und Application Control für die Internetschnittstelle beinhaltete. Aufgrund der stark zunehmenden Geschwindigkeiten wurden Firewalls für Rechenzentren (Data Center Firewalls, DCFW) entwickelt, die einen Durchsatz von über 100 GBit/s ermöglichen. Alle diese Firewalls arbeiten ausgehend von der Prämisse, dass der Schutz von außen nach innen erfolgt.

Um den Schutz intern schnell zu implementieren und zu gewährleisten sind, ist eine neue Art von Firewall erforderlich: die Internal Segmentation Firewall (ISFW). Die Internal Segmentation Firewall verfügt über einige Merkmale, die sie von herkömmlichen Firewalls unterscheidet. Die Unterschiede sind in Abbildung 2 dargestellt.

Grundlage der ISFW

Unternehmen sollten an strategischen Punkten im internen Netzwerk eine ISFW mit den neuesten Funktionen implementieren und somit eine zusätzliche Sicherheitsebene mit den folgenden Vorteilen einziehen:

- Kontrolle des Zugangs zu wichtigen Daten/Ressourcen möglichst nah am Benutzer über richtlinienbasierte Segmentierung.
- Einrichtung von Sicherheitsschranken, um durch fortschrittliche Sicherheitsmechanismen die unkontrollierte Ausbreitung von Bedrohungen und Hacker-Aktivitäten im internen Netzwerk zu beenden bzw. einzugrenzen.
- Begrenzung der möglichen Schäden durch Bedrohungen innerhalb der Perimetergrenzen.
- Mehr Sichtbarkeit von Bedrohungen und bessere Erkennung und Abwehr von Angriffen.
- Schärfung des Sicherheitsprofils des Unternehmens insgesamt

Implementierungs-modus	ISFW	NGFW	DCFW	UTM	CCFW
Zweck	Sichtbarkeit und Schutz für interne Segmente	Sichtbarkeit und Schutz vor externen Bedrohungen und Internetaktivitäten	Schutz von Netzwerken mit hoher Leistung, niedriger Latenz	Sichtbarkeit und Schutz vor externen Bedrohungen und Benutzeraktivitäten	Netzwerksicherheit für Service Provider
Standort	Access Layer	Internet-Gateway	Core Layer/DC-Gateway	Internet-Gateway	Verschiedenes
Netzwerkbetriebsmodus	Transparent-Modus	NAT/Routing-Modus	NAT/Routing-Modus	NAT/Routing-Modus	NAT/Routing-Modus
Hardwareanforderungen	Höhere Port-Dichte zum Schutz mehrerer Ressourcen	GbE- und 10-GbE-Ports	Hohe Geschwindigkeit (GbE/10 GbE/40 GbE/100) und hohe Port-Dichte, Hardware-beschleunigung	Hohe GbE-Port-Dichte, integrierte WLAN-Anschlüsse und POE	Hohe Geschwindigkeit (GbE/10 GbE/40 GbE) und hohe Port-Dichte, Hardwarebeschleunigung
Sicherheitskomponenten	Firewall, IPS, ATP, Application Control	(Benutzerbasiert) Firewall, VPN, IPS, Application Control	Firewall, DDoS-Schutz	Umfassend und erweiterbar, Client- und Geräteintegration	Firewall, CGN, LTE und mobile Sicherheit
Weitere Eigenschaften	Schnelle Implementierung – fast ohne Konfiguration	Integration mit Advanced Threat Protection (Sandbox)	Hohe Verfügbarkeit	Unterschiedliche WAN-Konnektivitätsoptionen, z. B. 3G4G	Hohe Verfügbarkeit

ABBILDUNG 2 – UNTERSCHIEDE ZWISCHEN VERSCHIEDENEN FIREWALLS

Die ISFW muss eine richtlinienbasierte Segmentierung bieten.

Mithilfe der richtlinienbasierten Segmentierung kann der Benutzerzugang zu Anwendungen und Ressourcen besser kontrolliert und segmentiert werden, indem die Identität des Benutzers mit der Durchsetzung bestimmter Sicherheitsrichtlinien verknüpft wird. Dank richtlinienbasierter Segmentierung können potenzielle durch den Benutzer eingeschleppte Angriffsvektoren und Bedrohungen eingrenzen.

Die richtlinienbasierte Segmentierung kann als automatische Verknüpfung der Benutzeridentität mit der geltenden Sicherheitsrichtlinie definiert werden. Die Identität eines Benutzers kann als eine Reihe von Attributen definiert werden, wie physischer Standort, Art des für den Zugang zum Netzwerk verwendeten Geräts, verwendete Anwendung usw. Da sich die Benutzeridentität dynamisch ändern kann, muss die geltende Sicherheitsrichtlinie dynamisch und automatisch der Benutzeridentität folgen.

Um die erforderliche Benutzeridentifizierung und die allgemeinen Parameter zu erhalten, die für die Erstellung und Durchsetzung granulärer Sicherheitsrichtlinien benötigt werden, muss die ISFW Folgendes können:

1. Identifizierung von Benutzer, Gerät und Anwendung zulassen
2. Einbindung in Lösungen für Verzeichnisdienste ermöglichen, um die Identität des Benutzers zu ermitteln
3. Dynamische Zuordnung der Benutzeridentität zu einer spezifischen Sicherheitsrichtlinie und Durchsetzung der Richtlinie

Die ISFW muss vollständigen Schutz bieten.

Das erste Element der Sicherheit ist Sichtbarkeit. Und Sichtbarkeit bedeutet nichts weiter, als über die Netzwerkpakete Bescheid zu wissen. Wie sieht ein Paketstrom für eine bestimmte Anwendung aus? Woher kam er, wohin geht er? Welche Aktionen werden ausgeführt (Download, Upload usw.)?

Das zweite und ebenso wichtige Element ist Schutz. Sind Anwendung, Inhalt oder die Aktionen bösartig? Darf diese Art von Datenverkehr von dieser Ressourcengruppe an eine andere Ressourcengruppe übermittelt werden? Auch wenn das über unterschiedliche Inhalts- und Anwendungstypen hinweg schwierig ist, ist es wesentlicher Bestandteil der ISFW. Eine bösartige Datei, Anwendung oder einen Exploit zu erkennen, gibt dem Unternehmen genug Zeit zum Reagieren und die Bedrohung einzudämmen. Damit sie schlagkräftig sind, müssen sich all diese Schutzelemente auf einem einzigen Gerät befinden.

Sowohl Sichtbarkeit als auch Schutz hängen stark von einem in Echtzeit arbeitenden zentralen Dienst zur Auswertung von Bedrohungsdaten ab. Eine Frage muss immer gestellt werden: Wie gut sind Sichtbarkeit und Schutz? Sind sie für die neusten Bedrohungen gewappnet? Deshalb sollten alle Sicherheitsservices kontinuierlich durch Drittanbieter getestet und zertifiziert werden.

Die ISFW muss leicht zu implementieren sein.

Die ISFW muss einfach zu implementieren und zu verwalten sein. Es der IT-Abteilung leicht zu machen bedeutet, dass die ISFW ohne großen Konfigurationsaufwand und ohne eine Veränderung der Architektur des bestehenden Netzwerks implementiert werden kann.

Die ISFW muss zudem in der Lage sein, unterschiedliche Arten interner Ressourcen zu schützen, die sich an verschiedenen Stellen des Netzwerks befinden. Beispielsweise eine Gruppe von Servern mit wertvollen Kundendaten oder eine Gruppe von Endgeräten, die nicht mit dem neuesten Sicherheitsschutz aktualisiert werden kann.

Außerdem muss gewährleistet sein, dass die ISFW mit anderen Komponenten der Sicherheitslösung des Unternehmens integriert werden kann. Weitere Sicherheitslösungen können noch zusätzliche Sichtbarkeit und zusätzlichen Schutz bieten. Dazu gehören E-Mail-Gateway, Web-Gateway, äußere Firewalls, Cloud-Firewalls und Endgeräte. Und alles zusammen muss über eine „zentralen Konsole“ verwaltet werden können. So können Sicherheitsrichtlinien an der Netzwerkgrenze, im Inneren des Netzwerks und sogar außerhalb des Netzwerks in den Clouds konsistent umgesetzt werden.

Zudem werden herkömmliche Firewalls meist als Router implementiert. Schnittstellen (Ports) sind mit IP-Adressen gut definiert. Deren Planung und Implementierung dauert oft Monate – wertvolle Zeit in unserer heutigen Welt der kontinuierlichen Cyberangriffe. Eine ISFW kann im Netzwerk schnell und ohne nennenswerte Unterbrechungen implementiert werden. Das muss so einfach sein, wie das Einschalten und Anschließen eines Geräts. Die Firewall muss für Netzwerk und Anwendung transparent sein.

Die Leistung der ISFW muss der Leitungsgeschwindigkeit entsprechen.

Da Internal Segmentation Firewalls zur Zonenabgrenzung im Netzwerk implementiert werden, müssen sie sehr leistungsfähig sein, um den Ansprüchen des internen bzw. „East-West-Traffic“ zu genügen und um sicherzustellen, dass sie an diesen kritischen Punkten nicht zu einem Engpass werden. Anders als Firewalls an der Netzwerkgrenze,

die für den Zugang zum Wide Area Network (WAN) oder zum Internet mit Geschwindigkeiten von unter 1 GBit/s zu tun haben, laufen interne Netzwerke mit mehreren Gigabit pro Sekunde viel schneller. Dort müssen ISFWs mit Geschwindigkeiten von mehreren Gigabit pro Sekunde arbeiten und eine detaillierte Überprüfung von Paketen/Verbindungen durchführen können, ohne das Netzwerk zu verlangsamen.

Anforderungen an die ISFW-Technologie

Ein flexibles Netzwerk-Betriebssystem

Fast alle Implementierungs-Modi für Firewalls erfordern die Zuweisung einer IP-Adresse und eine Neukonfiguration des Netzwerks. Das bezeichnet man als Netzwerk-Routing-Implementierung. Es macht den Datenverkehr sichtbar und schützt vor Bedrohungen. Auf der anderen Seite des Spektrums gibt es den „Sniffer-Modus“, der leichter zu konfigurieren ist und Sichtbarkeit, jedoch keinen Schutz bietet.

Der Transparent-Modus vereint die Vorteile von Netzwerk-Routing- und Sniffer-Modus. Er bietet eine schnelle Implementierung und Sichtbarkeit sowie – was besonders wichtig ist – Schutz. Die Unterschiede sind in Abbildung 3 zusammengefasst.

Implementierungsmodus	Komplexität der Implementierung	Netzwerkfunktionen	Hohe Verfügbarkeit	Sichtbarkeit des Datenverkehrs	Schutz vor Bedrohungen
Netzwerk-Routing	Hoch	L3-Routing	✓	✓	✓
Transparent	Niedrig	L2-Bridge	✓	✓	✓
Sniffer	Niedrig	X	X	✓	X

ABBILDUNG 3 – UNTERSCHIEDE ZWISCHEN VERSCHIEDENEN FIREWALLS

Eine skalierbare Hardware-Architektur

Da interne Netzwerke bei sehr viel höheren Geschwindigkeiten arbeiten, muss die Architektur von ISFWs beim Schutz auf einen Durchsatz von mehreren Gigabit pro Sekunde ausgelegt sein. Rein CPU-basierte Architekturen sind zwar flexibel, entwickeln sich aber bei hohen Durchsatzanforderungen zu Nadelöhren. Die überlegene Architektur verwendet aus Flexibilitätsgründen zwar noch immer eine CPU, ergänzt diese aber durch individuelle ASICs, um den Netzwerkverkehr und die Inhaltsprüfung zu beschleunigen.

Da die ISFW näher an den Daten und Geräten implementiert wird, muss sie gelegentlich mit schwierigeren Umgebungen zurechtkommen. Daher ist ein widerstandsfähigerer Formfaktor eine weitere Anforderung an ISFWs.

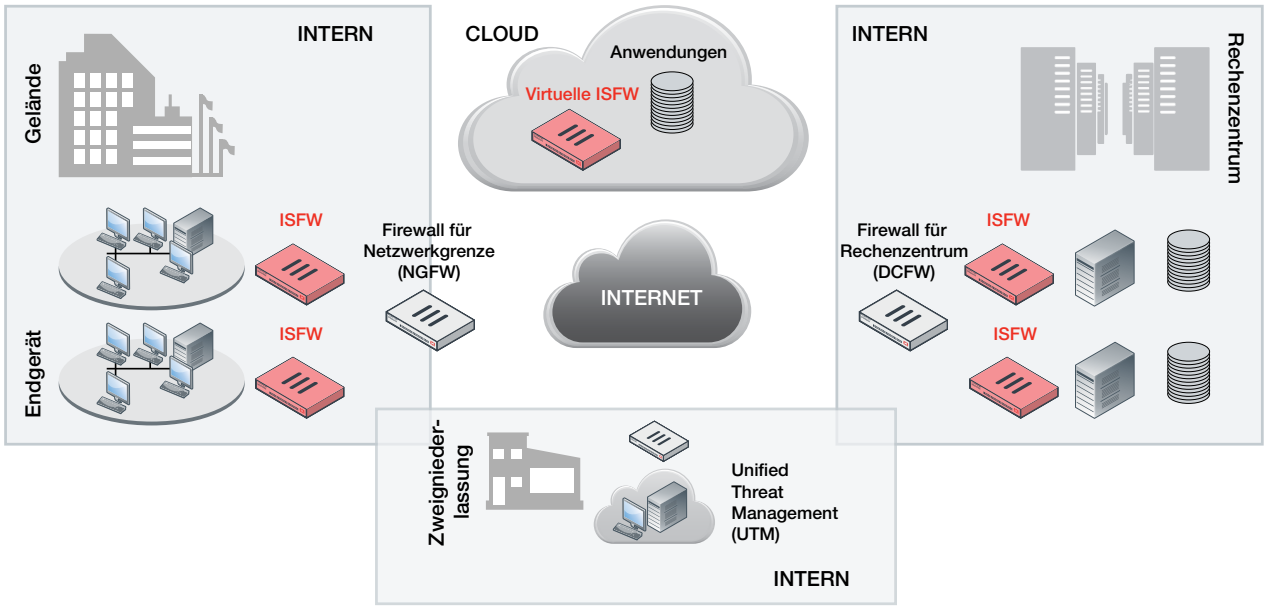


ABBILDUNG 4 – IMPLEMENTIERUNG EINER Internal Segmentation Firewall (ISFW)

Netzwerksegmentierung – integriertes High-Speed-Switching

Ein sich abzeichnender Aspekt des Transparent-Modus ist die Fähigkeit, Subnetzwerke und Server über einen Switch physisch zu trennen. Inzwischen gibt es auf dem Markt erste Firewalls mit voll funktionsfähigen integrierten Switches innerhalb der Appliance. Diese neuen Firewalls mit zahlreichen 10-GbE-Port-Schnittstellen entwickeln sich zu einer idealen „Top-of-Rack"-Lösung für Rechenzentren, die eine physische und virtuelle Sicherung von Servern erlaubt. Ähnliche Switch-integrierte Firewalls mit einer hohen Dichte an 1-GbE-Port-Schnittstellen werden zur idealen Lösung für die Trennung von LAN-Subsegmenten. ISFWs müssen in der Lage sein, beide Rollen zu erfüllen, und sollten daher idealerweise über umfassende integrierte Switching-Funktionen verfügen.

Echtzeit-Sicherheit

Internal Segmentation Firewalls müssen das volle Spektrum moderner Sicherheitsservices bereitstellen können, darunter IPS, Anwendungssichtbarkeit, Antivirus, Antispam sowie die Integration von cloudbasiertem Sandboxing, und müssen die Durchsetzung von Richtlinien ermöglichen, die die äußeren Standard-Firewalls ergänzen. Diese Sichtbarkeit und der Schutz in Echtzeit sind entscheidend, um die Ausbreitung von Malware im Netzwerk zu begrenzen.

Beispiel für die netzwerkweite Implementierung einer ISFW

Die meisten Unternehmen schützen ihre Netzwerkgrenze mit Firewalls, NGFWs und UTMs. Das sind immer noch wichtige Bestandteile des Netzwerkschutzes. Um das Sicherheitsniveau anzuheben, können intern jedoch auch Internal Segmentation Firewalls strategisch platziert werden. Dabei könnte eine bestimmte Gruppe von Endgeräten betreffen, bei denen Sicherheits-Updates schwierig sind, oder Server, auf denen sich geistiges Eigentum befindet.

Beispiel für die Segmentierung einer ISFW-Implementierung

Die ISFW wird meist im Access Layer (Datenzugriffsschicht) implementiert und schützt eine bestimmte Ressourcengruppe. Anfänglich ist die Implementierung zwischen dem Verteilungs- und dem Zugangs-Switch transparent. Langfristig könnte das integrierte Switching an die Stelle von Zugangs- und Verteilungs-Switch treten und zusätzlichen physischen Schutz bieten.

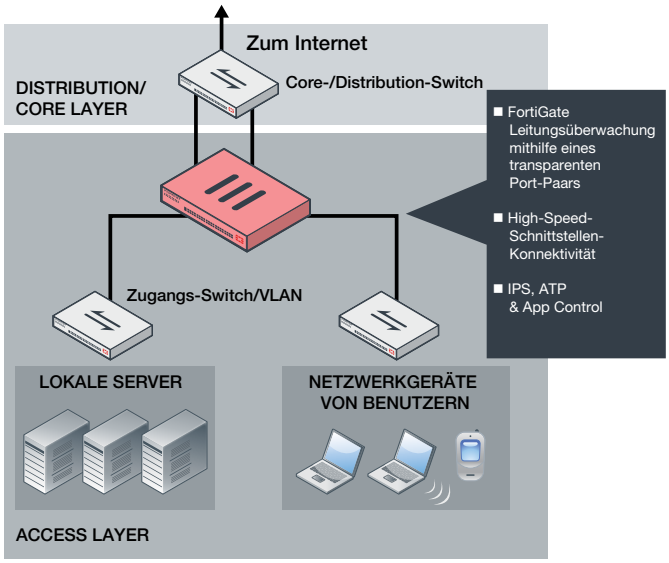


ABBILDUNG 5 – IMPLEMENTIERUNG EINER INTERNAL SEGMENTATION FIREWALL (ISFW)

Optimierung von Advanced Threat Protection mit interner Sichtbarkeit

Ein erfolgversprechender Ansatz zur Abwehr komplexer Bedrohungen muss einen kontinuierlichen Zyklus aus Vorbeugen, Erkennen und Abwehren umfassen. Sehr typisch wäre eine Next Generation Firewall (NGFW) als wichtige Basis der Präventionskomponente, die eine L2/L3-Firewall, Intrusion Prevention, Application Control und mehr ermöglicht, um bekannte Bedrohungen abzuwehren und gleichzeitig unbekannte stark risikobehaftete Elemente zur Erkennung in eine Sandbox durchzuleiten. Da NGFWs jedoch traditionell am Netzwerkrand implementiert werden, machen sie den Angriffszyklus nur teilweise sichtbar, da sie primär Eingangs- und Ausgangsaktivitäten beobachten.

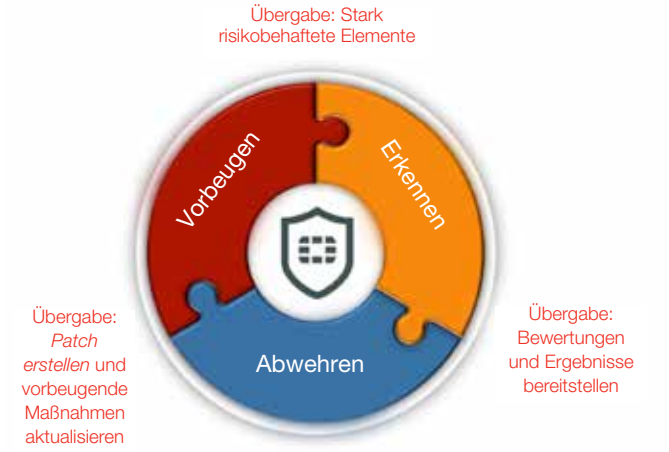


ABBILDUNG 6 – ADVANCED THREAT PROTECTION (ATP) FRAMEWORK

Die Implementierung einer ISFW kann zusätzlich ein umfassenderes Bild Hacker-Aktivitäten bieten, nachdem sie die Netzwerkgrenze überwunden haben. Querbewegungen können einen erheblichen Anteil der bösartigen Aktivitäten ausmachen, wenn Hacker versuchen, wertvolle Ressourcen zu ermitteln und Daten abzugreifen. Ein umfassenderes Bild der Aktivitäten im Inneren des Netzwerks und an dessen Rand verbessert alle Phasen eines vollständigen ATP Framework. Die Bandbreite des internen Netzwerkverkehrs ist häufig um ein Vielfaches höher als die des Randverkehrs. Daher kann eine ISFW die Ausbreitung von bekannten Techniken ausgehender Gefährdungen viel effektiver begrenzen und stärker risikobehaftete Elemente für eine eingehendere Untersuchung an Sandboxes weiterleiten.

Fazit

Komplexe Bedrohungen nutzen das „flache interne“ Netzwerk aus Sobald der äußere Verteidigungswall überwunden wurde, ist die Ausbreitung der Bedrohung und schließlich die gezielte Abschöpfung wertvoller Daten kaum noch aufzuhalten. Da die Architektur herkömmlicher Firewalls für die geringeren Geschwindigkeiten der Internetschnittstelle ausgelegt ist, können diese Sicherheitsgeräte nur schwer intern eingesetzt werden. Darüber hinaus dauert die Implementierung von Firewall-Netzwerkkonfigurationen (IP-Adressen) lange.

Internal Segmentation Firewalls sind eine neue Art von Firewall, die schnell und ohne nennenswerte Unterbrechungen implementiert werden können und dabei die Geschwindigkeiten interner Netzwerke von mehreren Gigabit pro Sekunde aufrechterhalten können. Bestimmte Teile des internen Netzwerks können sofort mit Sichtbarkeit und Schutz ausgestattet werden.

FORTINET

DEUTSCHLAND
Feldbergstraße 35
60323 Frankfurt
Deutschland
Verkaufsabteilung: +49 69 310 192 0

SCHWEIZ
Riedmuehlestr. 8
CH-8305 Dietlikon/Zürich
Schweiz
Verkaufsabteilung: +41 44 833 68 48

VERTRIEBSBÜRO APAC
300 Beach Road 20-01
The Concourse
Singapur 199555
Tel.: +65 6513 3730

ÖSTERREICH
Wienerbergstrasse 7/D/12th floor
1100 Wien
Österreich
Verkaufsabteilung: +43 1 22787 120

KONZERNSITZ
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
USA
Tel.: +1 (408) 235 7700
www.fortinet.com/sales

VERTRIEBSBÜRO EMEA
120 rue Albert Caquot
06560, Sophia Antipolis,
Frankreich
Tel.: +33 (0)4 8987 0510

VERTRIEBSBÜRO LATEINAMERIKA
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel.: +52 (55) 5524 8480