WHITE PAPER

Leitfaden für die absichtsbasierte Segmentierung

Grundlegende Verfahren zur Risikoabwehr und Compliance – über die gesamte Angriffsfläche hinweg

Executive Summary

Die Segmentierung von Netzwerken, Geräten, Benutzern und Anwendungen ist seit langem ein Best Practice zum verstärkten Schutz des Netzwerkrands und zum Aufbrechen flacher Netzwerktopologien. Für die Verantwortlichen von Netzwerktechnik und -betrieb, die Risikoabwehr, Compliance und die effektive Verwaltung des Sicherheitsprofils im Auge haben, sind die aktuellen Segmentierungsansätze jedoch unzureichend.

Herkömmliche Ansätze kontrollieren den Zugriff auf eine Ebene, die zu grobkörnig ist, um die Geschäftsanforderungen zu erfüllen. Sie stützen sich auf Gefahrenbewertungen, die schnell veraltet sind, und gehen davon aus, dass ein Schutz vor Bedrohungen besteht, selbst wenn das Unternehmen klaffende Lücken in seiner wachsenden Angriffsfläche aufweist. In diesee Umgebung können die Netzwerk-Verantwortlichen den Sicherheitsstatus nicht proaktiv managen, wodurch die Organisation größeren Sicherheitsrisiken ausgesetzt wird.

Angesichts aufgeblähter Angriffsflächen durch Multi Cloud, Mobile First, das Internet der Dinge (IoT) und andere digitale Transformationsinitiativen bietet die absichtsbasierte Segmentierung einen wichtigen neuen Ansatz. Sie behebt die aktuellen Defizite der Segmentierung und kann bei einer Vielzahl von Zugangskontroll-Szenarien eingesetzt werden.

Wie können Unternehmen mit durchschnittlich 75 verschiedenen Sicherheitstools eine transparente, durchgängige End-to-End-Transparenz erwarten?[1]

Eine effektive Segmentierung muss die Geschäftsabsicht nutzen, um das Wo, Wie und Was für eine effektive Sicherheit festzulegen.

Grundlagen der absichtsbasierten Segmentierung

Die absichtsbasierte Segmentierung übersetzt die Geschäftsabsicht des Netzwerkverantwortlichen in das „Wo“, „Wie“ und „Was“ der Security-Segmentierung:

- **„Wo“** legt die Standorte der Segmentabgrenzung und die Logik fest, nach der die IT-Assets segmentiert werden.
- **„Wie“** implementiert die Geschäftsabsicht mit feinmaschiger Zugangskontrolle und verwaltet sie basierend auf kontinuierlichem, adaptivem Vertrauen.
- **„Was“** erzwingt die Zugangskontrolle durch die Anwendung leistungsstarker, moderner Sicherheit (Layer 7) über das gesamte Netzwerk hinweg.

Diese drei Elemente sind im Kontext einer integrierten Fabric von Sicherheitskomponenten, die sich mit anderen Netzwerk- und Infrastrukturgeräten verbinden und mit diesen kommunizieren, entscheidend. Netzwerkverantwortliche können so ohne Änderung ihrer Architekturen ihren Sicherheitsstatus effektiv verbessern, Risiken abwehren und Compliance und Betriebseffizienz über das gesamte Unternehmen hinweg unterstützen.

Segmentierung, die dem Geschäftszweck gerecht wird

Absichtsbasierte Segmentierung unterstützt vorherrschende **Architekturen mit Makro- und Mikrosegmentierung** sowie die **Segmentierung auf Anwendungs-, Prozess- und Endgeräteebene**. Durch die Segmentierung eines flachen Netzwerks mit einer dieser Segmentierungstechniken kann ein Netzwerkbetreiber kleinere, besser kontrollierbare Angriffsflächen schaffen, die durch leistungsfähige moderne Security-Komponenten (Layer 7) weiter geschützt werden können.

Absichtsbasierte Segmentierung ermöglicht es Netzwerkbetreibern, Security-Domains oder -Segmente zu schaffen, die dem jeweiligen Geschäftszweck entsprechen. Um die Geschäftsabsicht zu erreichen, muss die Segmentierung jedoch eine granularere Zugriffskontrolle bereitstellen, die auf der **Benutzeridentität oder einer Geschäftslogik** basiert. Sie muss die Möglichkeit bieten, die Zugriffskontrolle auf der Grundlage des aktuellen Vertrauens anzupassen, indem eine externe Vertrauensdatenbank abgefragt wird, die eine kontinuierliche Bewertung erfasst.

Adaptives Vertrauen für ein fundiertes Risiko-Management

Traditionell wird bei der Zugangskontrolle von unveränderlichen Vertrauensstufen für Benutzer, Geräte und Anwendungen ausgegangen. Tatsächlich ändert sich die Vertrauenswürdigkeit all dieser Elemente jedoch häufig, entweder durch normale Änderungen im Geschäftsbetrieb oder durch die veränderte Bedrohungen. Da Änderungen der Vertrauensstufe den Sicherheitsstatus einer Organisation und das inhärente Risiko des Netzwerks drastisch beeinflussen, führt die Verwendung von statischen Vertrauensstufen dazu, dass die Netzwerkverantwortlichen gefährlich uninformiert sein könnten.

Aus diesem Grund verknüpft die absichtsbasierte Segmentierung die Zugangskontrolle mit kontinuierlich aktualisierten Vertrauensstufen. Bei den umfassenderen absichtsbasierten Segmentierungslösungen werden diese Informationen sowohl aus internen als auch aus externen Quellen bezogen.

Absichtsbasierte Segmentierung ermöglicht nicht nur ein genaueres Bild der inhärenten Risiken des Netzwerks, sondern bietet auch die Fähigkeit, den Sicherheitsstatus kontinuierlich zu bewerten. Mit den **Security Rating Services** werden aussagekräftige Einblicke in die Risiken und Schwachstellen gewonnen, Best Practices zur Behebung von Konfigurationsdefiziten bereitgestellt und wird die Sicherheitskonfiguration des Netzwerks bewertet. Diese Dienste verfolgen auch den Sicherheitsstatua über längere Zeit, vergleichen den gesamten Sicherheitsstatus der Organisation mit dem ähnlicher Organisationen und bewerten ihn anhand anerkannter Sicherheitsstandards. Unternehmen sollten nach Threat Intelligence-Lösungen suchen, die Funktionen zur Security-Bewertung in Echtzeit bereitstellen und ihnen über eine zentrale Konsole vollständige Transparenz der Schwachstellen bieten. Mithilfe der Funktionen zur Security-Bewertung können Netzwerk-Teams das Schließen von Sicherheitslücken priorisieren und bei Änderungen neue Bedrohungen identifizieren – sowohl innerhalb des Netzwerks als auch außerhalb.

72 % des Internet-Verkehrs ist inzwischen verschlüsselt, und Cyber-Kriminelle nutzen das aus, um Netzwerke zu infiltrieren und Daten zu extrahieren.

Aufgrund der komplexen Bedrohungslandschaft müssen die Netzwerk-Verantwortlichen den Sicherheitsstatus ihres Netzwerks kontinuierlich prüfen und bewerten.

Leistungsstarker, allgegenwärtiger Schutz vor Bedrohungen

Viele Unternehmen, die Zugangskontrollen implementieren, verfügen nicht über alle notwendigen Sicherheitskomponenten, um diese auch durchzusetzen, und die vorhandenen Komponenten sind nicht immer integriert. Dies schränkt die Möglichkeiten der Netzwerk-Verantwortlichen ein, neue Bedrohungen zu erkennen und zu verhindern, dass Angriffe ihre Ziele erreichen oder das gesamte Netzwerk infizieren.

Always-On SSL im gesamten Netzwerk. Um die Zugriffsrichtlinien durchzusetzen und die gesamte Angriffsfläche zu verteidigen, schreibt absichtsbasierte Segmentierung einen äußerst kostengünstigen und leistungsstarken Bedrohungsschutz (Layer 7) in Next Generation Firewalls (NGFWs) vor, der eine Secure Socket Layer-(SSL)-Prüfung als integrierte Komponente bereitstellt.

Da 72 % des Internet-Verkehrs inzwischen verschlüsselt ist, ist die Prüfung des SSL- oder TLS-(Transport Layer Security-)verschlüsselten Datenverkehrs im gesamten Netzwerk nicht mehr optional.[2] Malware wie Heartbleed, Poodle und Zeus hat gezeigt, wie anfällig der Verschlüsselungsstandard für die Ausnutzung ist.[3] Dennoch zögern viele Unternehmen, die SSL-Prüfung in vollem Umfang anzuwenden, da sie sich auf den Netzwerkdurchsatz und die Benutzererfahrung auswirken kann. Aus diesem Grund sollten die in der absichtsbasierten Segmentierung verwendeten NGFWs über **spezielle leistungsfähige Prozessoren** verfügen, die die Beeinträchtigung des Durchsatzes minimieren. Bei der Verwendung solcher Prozessoren kann die SSL-Prüfung in allen NGFWs immer aktiviert sein.

Ein wichtiges Prinzip der absichtsbasierten Segmentierung ist die Möglichkeit, den Schutz überall dort bereitzustellen, wo er benötigt wird, sowohl On-Premise als auch in allen vom Unternehmen genutzten Clouds. Manche Netzwerk-Verantwortlichen sträuben sich gegen die potenziellen Kosten einer solchen Richtlinie. Die Wahl von NGFWs von einem Anbieter, der eine Vielzahl von physischen und virtuellen Formfaktoren und Port-Dichten anbietet, minimiert die Gesamtbetriebskosten (TCO) und macht eine flächendeckende Implementierung möglich.

End-to-End-Management. Wenn über das Netzwerk hinweg unterschiedliche Threat Protection-Lösungen implementiert werden, ist eine effektive End-to-End-Transparenz und -Verwaltung erforderlich. Um das gesamte Netzwerk proaktiv vor Bedrohungen zu schützen, die von irgendeinem Netzwerkbereich ausgehen, sollten absichtsbasierte Segmentierungslösungen als Teil einer integrierten Security Fabric implementiert werden. In diesem Fall muss diese eine umfassende, durchgängige Transparenz und konsistente Richtlinienkontrollen über alle Sicherheitseinrichtungen hinweg bieten.

Anwendungsfälle

Absichtsbasierte Segmentierung kann in einer Vielzahl von Zugangskontroll-Szenarien angewendet werden. Nachfolgend finden Sie zwei Beispiele, die veranschaulichen, wie geeignete Klassifizierungen der Zugangskontrolle und fortschrittlicher, leistungsstarker Bedrohungsschutz den Verantwortlichen bessere Kontrolle über ihre Sicherheitsarchitektur bieten und ihnen helfen, Risiken effektiver abzuwehren.

Anwendungsfall: Reduzierung der Angriffsfläche

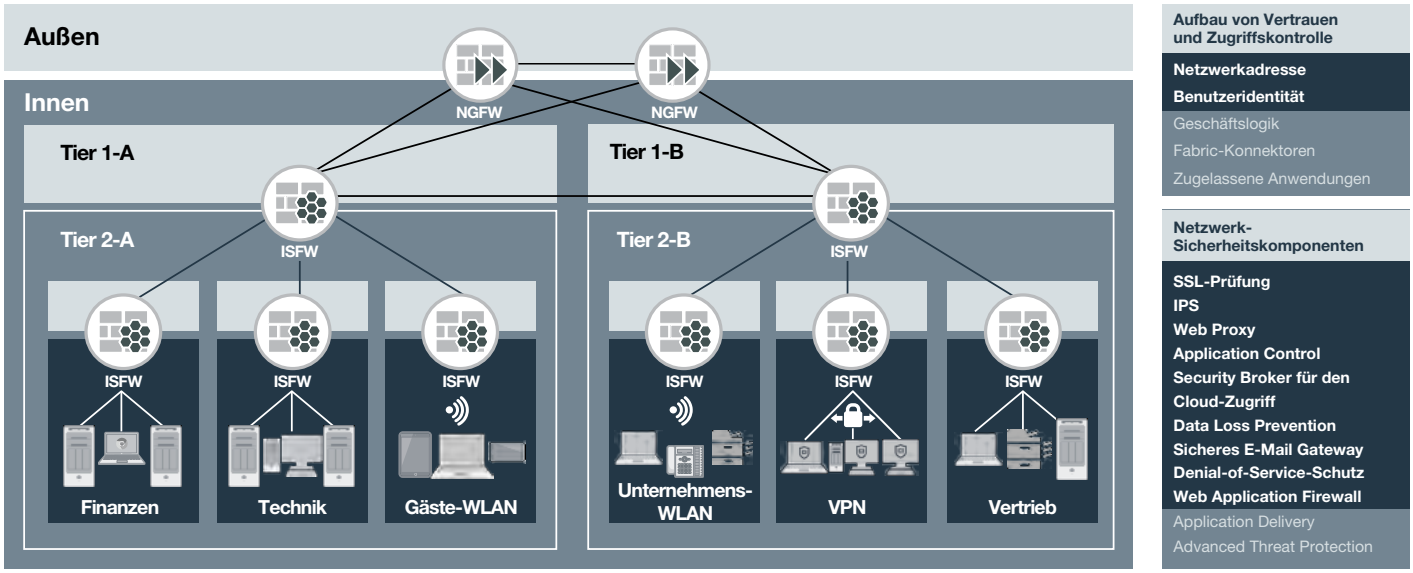

Abbildung 1. Anwendungsfall: Risikominderung durch Reduzierung der Angriffsfläche

Die meisten Unternehmen können sich beim Schutz ihrer Netzwerk-Assets nicht alleine auf das Sichern des Perimeters verlassen. Wenn es zu Datenschutzverletzungen kommt – aufgrund von unsachgemäßer Konfiguration, infizierten Geräten, die mit dem internen Netzwerk verbunden sind, oder Zero-Day-Angriffen, die Security Controls umgehen – muss das Netzwerk mit **zusätzlichen Verteidigungsstufen** ausgestattet sein (siehe Abbildung 1 an den Grenzen zwischen Tier 1 und 2 sowie innerhalb Tier 2).

Diese zusätzlichen internen Segmentation Firewalls wenden eine Vielzahl von Security Controls an, um jede böswillige Aktivität innerhalb der von ihnen geschützten Zonen einzudämmen. Die Authentifizierung basiert in diesem Fall gewöhnlich auf der Asset-ID (Netzwerkadresse) oder der Benutzeridentität. Beachten Sie, dass das Hinzufügen der Sicherheitssegmentierung keine Änderung der Netzwerkarchitektur selbst erfordert.

Alle Firewalls kommunizieren miteinander und mit der zentralen Konsole des Management-Systems, was zu einer durchgängigen Transparenz des Datenverkehrs führt. Das Fabric-basierte Management-System konsolidiert die Threat Protection-Aktivitäten aller Sicherheitskomponenten und erstellt einen vollständigen Audit-Trail.

Anwendungsfall: Compliance

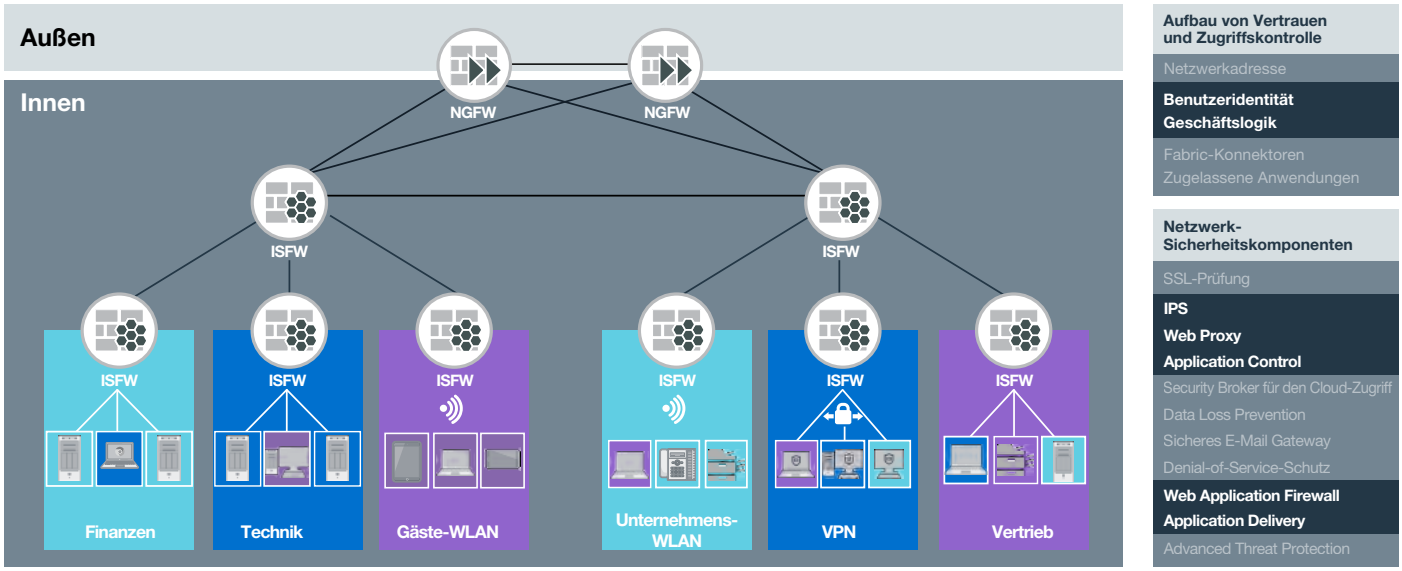

Abbildung 2. Anwendungsfall: Reaktion auf ein komplexes Gefüge von Compliance-Anforderungen

Compliance mit gesetzlichen und branchenspezifischen Vorschriften ist selten optional. Es ist jedoch unpraktisch, das Netzwerk jedes Mal neu zu konfigurieren, wenn sich Compliance-Regeln ändern oder neue Vorschriften in Kraft treten.

So wäre es beispielsweise äußerst schwierig, Assets für die Compliance mit dem Payment Card Industry Data Security Standard (PCI DSS) zu segmentieren, indem man nur das in Abbildung 2 dargestellte Finanzen-Sub-Netz isoliert. In realen Organisationen unterliegen möglicherweise nicht alle Geräte im Finanzen-Subnetz der Compliance mit dem PCI-Standard. Einige, die dem PCI-Standard unterliegen, befinden sich möglicherweise in anderen Sub-Netzen oder sogar an entfernten Standorten.

Mit der absichtsbasierten Segmentierung können Zugriffsrichtlinien definiert und durch die über die Fabric verbundenen Security-Komponenten durchgesetzt werden. Assets und Benutzer können für PCI-Compliance-Anforderungen gekennzeichnet werden, unabhängig von ihrem Standort im Netzwerk und unabhängig von anderen auf sie zutreffenden Compliance-Controls oder Zugriffsrichtlinien.

Fazit

Die absichtsbasierte Segmentierung ist zwar ein neuer Ansatz, aber dennoch eine reife Lösung. Die für die Implementierung der absichtsbasierten Segmentierung erforderlichen Produkte und Dienste sind allgemein verfügbar und die Liste der mit der Fabric verbundenen Threat Protection-Komponenten wächst stetig.

Netzwerk-Verantwortlichen wird empfohlen, Proof of Concepts für die absichtsbasierte Segmentierung zu implementieren, entweder indem sie die hier dargestellten Anwendungsfälle befolgen oder ihre eigenen Geschäftsanforderungen zugrunde legen. Auf Anfrage zeigt Fortinet, wie ein schrittweiser, messbarer Ansatz für die absichtsbasierte Segmentierung erfolgt werden kann, indem Kernkomponenten implementiert und mit den bereits vorhandenen Netzwerktechnologien des Unternehmens verbunden werden.

[1] Kacy Zurkus, „Defense in depth: Stop spending, start consolidating“, CSO Online, 14. März 2016.

[2] „Q3 2018 Threat Landscape Report“, Fortinet, 6. November 2018.

[3] Ananda Rajagopal, „How SSL encryption gives a false sense of security“, CSO Online, letzter Zugriff 4. Februar 2019.

FORTINET

www.fortinet.com

348072-0-1-DE Mai 15, 2019 2:05 nachm.

D:\00_projects\03_Argos_Multingual\542_A-341182-923463_Fortinet_DE\03_dtp\Various\WP_a-network\Asset\WP-Solution-research-network-director-A4\WP-Solution-research-network-director-A4