Forefront Threat Management Gateway (TMG) Whitepaper Die Lösung…

Einführung

Im vergangenen Jahr gab Microsoft Änderungen an den Roadmaps mehrerer Forefront-Produkte bekannt, unter anderem die Einstellung von Forefront Threat Management Gateway 2010 (TMG).

Der Grund für diese überraschende Änderung liegt laut Microsoft in der Absicht, seine Sicherheits- und Datenschutzlösungen besser auf die zu schützenden Workloads und Anwendungen auszurichten.

Welche Ersatzlösung steht für TMG bereit? Obwohl Microsoft sich die Migration von Sicherheitsservices in die Cloud rasch zu Eigen machte und dies auch seinen Kunden empfiehlt, stehen viele Unternehmen der Cloud zurückhaltend gegenüber und bevorzugen weiterhin einen „bodenständigen" Ansatz für ihr Netzwerksicherheitssystem, das sich einfach verwalten und steuern lässt.

Als Microsoft Global Alliance Partner bzw. vollständig zertifizierter Partner für Hardware-Lastverteilung bieten Dell SonicWALL und KEMP Technologies eine einzigartige Palette an integrierten Lösungen, die einen schnellen und einfachen Ersatz von Microsoft Forefront TMG-Systemen bzw. die Erweiterung bestehender Microsoft-Implementierungen für Unternehmen jeder Größe ermöglichen.

Wichtige Faktoren

Wenn Sie gegenwärtig TMG implementiert haben oder eine Einführung von TMG vor der Bekanntgabe der Abkündigung durch Microsoft geplant war, haben Dell SonicWALL und KEMP Technologies mit folgendem Angebot möglicherweise die passende Lösung für Sie:

- Firewall
- Lastverteilung
- Proxy
- Reverse Proxy
- Inhaltsfilterung
- Anti-Malware
- Site-to-Site-VPN
- Remote-Zugriff
- Hochverfügbarkeit

Darüber hinaus bieten KEMP Technologies und Dell SonicWALL Next Generation Firewalls:

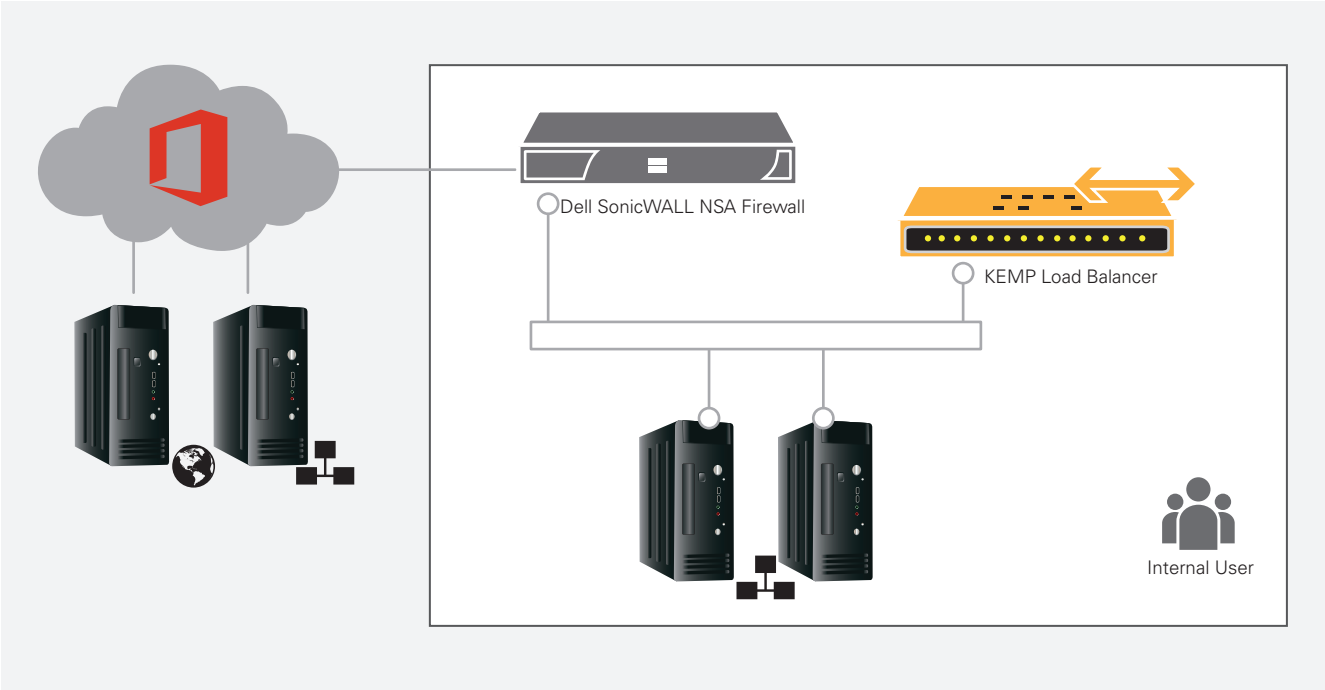
- Vollständige Layer 7-Anwendungsidentifikation und -kontrolle
- Intrusion Prevention
- Drahtlose(r) Zugang/Steuerung
- ISP-Redundanz und -Lastverteilung
- Echtzeitüberwachung
- Transparente Benutzerauthentifizierung und Richtlinienumsetzung
- WAN-Beschleunigung
- SSL-Inspektion
- Fernzugriff per IPSec- und SSL-VPN

Dell SonicWALL und KEMP Technologies haben Lösungspakete für die Anforderungen kleiner, mittelständischer und großer Unternehmen entwickelt. Die folgenden Lösungsbeispiele erstrecken sich über ein breites Spektrum an Unternehmen, in denen normalerweise Microsoft TMG mit einem umfangreichen Servicepaket zum Einsatz kommen würde.

Lösungen für kleinere Unternehmen

Viele kleine Unternehmen stellen gegenwärtig von herkömmlichen Systemen auf Cloud-Services wie Office 365 um, wodurch Sicherheit, Berechenbarkeit und Zuverlässigkeit zu zentralen Kriterien beim Zugriff auf lokale und entfernte Ressourcen und Anwendungen werden. Abbildung 1 zeigt eine typische Netzwerkimplementierung für ein kleines Unternehmen, das Cloud-Services über lokale Microsoft ADFS nutzt. Die Internetkonnektivität ist damit zu einer geschäftskritischen Komponente des Netzwerks geworden, da sie den Zugang zu den Geschäftsanwendungen und -daten erst ermöglicht.

Abbildung 1



Mit Dell SonicWALL-Firewalls profitieren Unternehmen von sicherer VPN-Konnektivität mit Cloud-basierten Services sowie dynamischem Bandbreitenmanagement für Anwendungen, einschließlich der Cloud-Services. Die Unterstützung mehrerer WAN-Verbindungen verbessert die Ausfallsicherheit und Zuverlässigkeit und gewährleistet den Zugang zu Daten und Anwendungen bei Übertragungsstörungen. Dell SonicWALL ermöglicht darüber hinaus die sichere Überwachung des Netzwerktraffics, um Viren, Spyware, Trojaner, Eindringlinge, Website-Zugriffskontrollen und zahlreiche weitere internetbasierte Bedrohungen aufzuspüren. Die gesamte Funktionalität wird auf einer einzelnen Hardwareplattform bereitgestellt, die als Standalone-System oder Hochverfügbarkeitspaar konfiguriert werden kann.

Dank der einfachen Bereitstellung und Verwaltung eignen sich Dell SonicWall-Firewalls ideal für kleine Unternehmen, die trotz begrenzter technischer Ressourcen eine Lösung mit vollem Funktionsumfang benötigen.

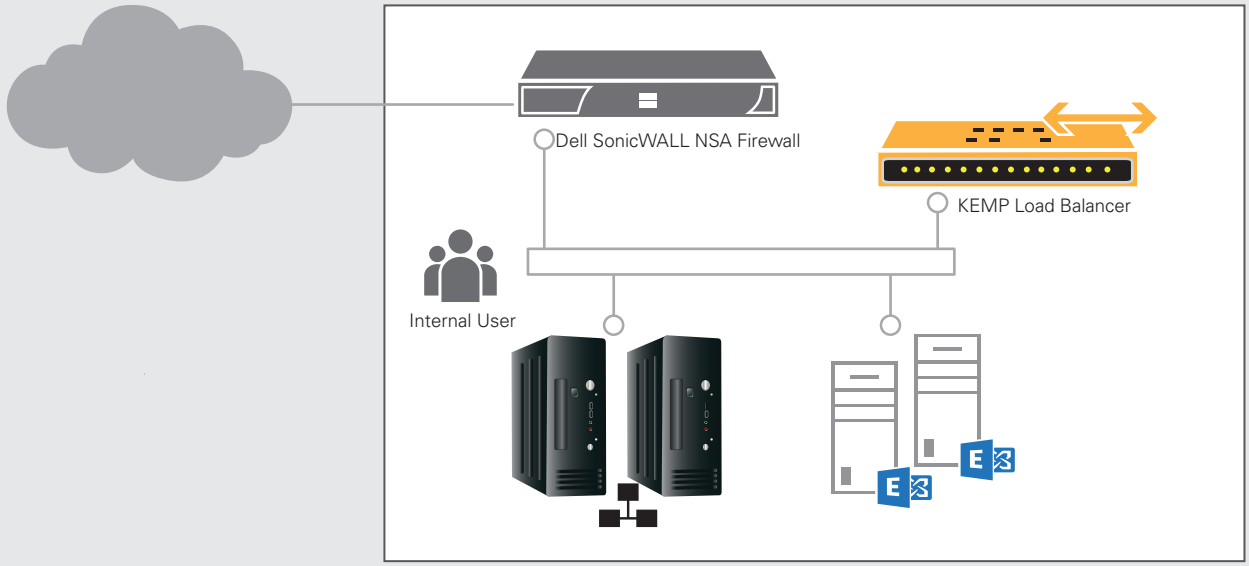
KEMP Technologies bietet Lösungen für Netzwerke in KMU- und Enterprise-Umgebungen, die mit integrierter Lastverteilung zwischen mehreren Anwendungsservern sowie der Ausfallsicherheit von Standorten eine sichere, zuverlässige Konnektivität für unternehmenskritische Dienste gewährleisten.

Microsoft ADFS und lokale Exchange-Services

Bei dieser Beispielimplementierung setzt der Kunde Microsoft ADFS für anspruchsbasierte Authentifizierung in der vorhandenen Exchange 2010-Infrastruktur sowie für anwendungsübergreifende Single Sign-on-Funktionalität (SSO) ein.

Weitere Dienste sind u. a. der interne und remote Zugriff auf die Outlook Web App (OWA) über die interne ADFS-Farm, wobei der KEMP LoadMaster in beiden Fällen für die Lastverteilung sorgt.

Abbildung 2



Der KEMP LoadMaster kombiniert Vielseitigkeit mit Benutzerfreundlichkeit und beschleunigt die Bereitstellung für die gesamte Palette an erweiterten Messaging-Anwendungen und -Protokollen, die von vielen Anwendungen, einschließlich Exchange 2010, verwendet werden.
Unterstützt werden die Outlook Web App (OWA), Outlook Anywhere (OA), ActiveSync (EAS), Simple Mail Transfer Protocol (SMTP), Post Office Protocol Version 3 (POP3), Internet Message Access Protocol Version 4 (IMAP4) sowie RPC Client Access (RPC CA).

Mit integrierter SSL-Beschleunigung und/oder Overlay verlagert der LoadMaster eine Hauptquelle der CPU-Last, um die Kapazität der Server zu verbessern. Die Layer 7-Integritätsprüfung im LoadMaster stellt sicher, dass bei Ausfall eines Servers der Load Balancer den Server offline nimmt und die Benutzer automatisch zu anderen funktionierenden Servern umleitet und mit diesen verbindet.

Die gesamte KEMP LoadMaster-Produktfamilie, einschließlich Virtual LoadMaster (VLM), unterstützt Microsoft-Workloads (Exchange, Lync, RDS und SharePoint) und andere Umgebungen wie HTTP/HTTPS, SQL, Oracle, Citrix und beinhaltet umfangreiche Garantieleistungen im ersten Jahr sowie technischen Support.

Dell SonicWall ist in der Lage, Kunden jeder Größenordnung eine passende Lösung anzubieten, die auf die Herausforderungen einer zunehmenden Netzwerkkomplexität abgestimmt ist. Alle unsere Firewalls sind mit derselben Betriebssoftware, SonicOS, ausgestattet und stellen dieselben Kernfunktionen bereit: traditionelle Stateful-Firewall, VPN, Website-Filterung, Intrusion Prevention, vollständige Layer 7-Anwendungskontrolle, Gateway-Virenschutz, Gateway-Anti-Spyware etc. Bei der Sicherheit und dem Funktionsumfang für kleine Unternehmen machen wir keine Kompromisse.

Um den steigenden Ansprüchen der Unternehmen gerecht zu werden, sind eine hohe Ausfallsicherheit und Redundanz des Netzwerks unabdingbar. Dell SonicWALL bietet kosteneffektive Optionen wie Hochverfügbarkeit und WAN-Failover, die einen ausfallsicheren Hardwarebetrieb ohne „Single-Point-of-Failure“ gewährleisten.

Lösungen für mittelständische und große Unternehmen

Einzelnetzwerke

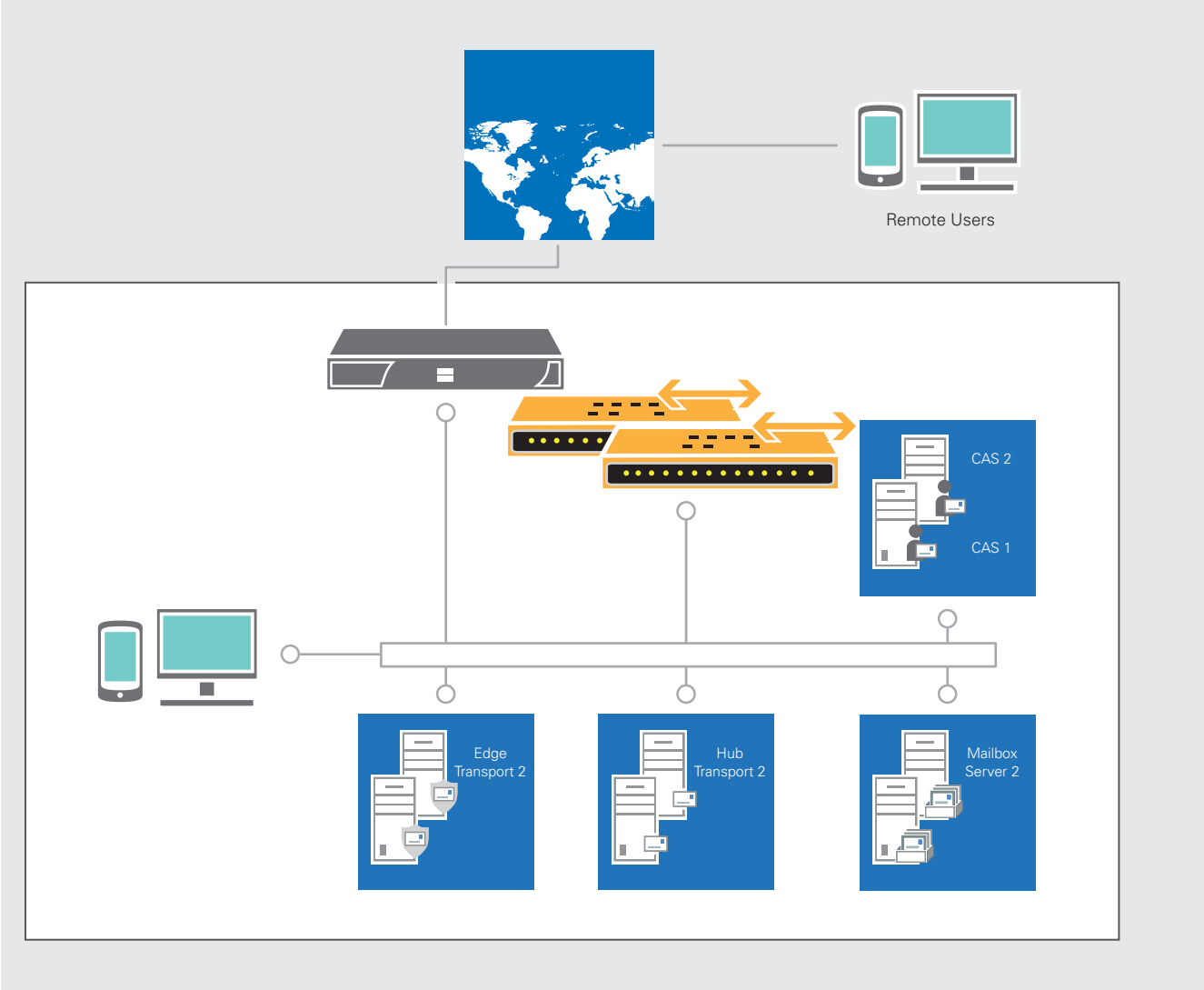
Mittlere und große Unternehmen haben tendenziell komplexere Netzwerke mit gemischten Implementierungsszenarien – lokal, Private, Public und Hybrid Cloud – und zahlreichen Anwendungen, die von einer breiten Benutzerbasis genutzt werden.

Sicherheit, Performance, Verfügbarkeit und Ausfallsicherheit müssen höchsten Ansprüchen genügen, da der Ausfall eines einzelnen Service oder nicht verfügbare Daten die Geschäftsabläufe erheblich beeinträchtigen können. Dell SonicWALL Next Generation Firewalls vereinen die bewährten Kernfunktionen mit einem gemeinsamen Betriebssystem in allen Bereichen – von der SOHO-Umgebung bis zum Rechenzentrum. Ob es sich um eine Einzelimplementierung im Head Office oder mehrere Standorte in einem verteilten VPN-Netzwerk mit mehreren Zweigstellen handelt, Dell SonicWALL hält stets die geeignete Lösung bereit.

Die NSA-Firewalls mit den Modellen NSA 4600 bis NSA 6600 gewährleistet unübertroffene Performance und Skalierbarkeit für Deep Packet Inspection, SSL-Inspektion, Anwendungsidentifikation und -kontrolle und Anti-Malware. Zusammen mit zahlreichen weiteren Services wie Remote-Zugriff, Site-to-Site VPN etc. bietet die NSA-Serie die perfekte Kombination aus Performance, Funktionalität und Preis.

Das Netzwerk in Abbildung 3 ist eine einzelne Zone (keine DMZ) mit einer begrenzten Anzahl an Anwendungen, die ausfallsicher sein müssen. Um Betriebsunterbrechungen zu vermeiden, müssen Sicherheit und Lastverteilung ein integraler Bestandteil der Netzwerktopologie sein. Zur Lastverteilung mehrerer Anwendungen mit denselben Geräten können kosteneffektive Lösungen implementiert werden, die eine konsistente, parallele Konnektivität mit mehreren Services gewährleisten.

Abbildung 3



In diesem Beispiel erfordern eine größere Benutzerbasis und schnellere Internetkonnektivität besonders hochleistungsfähige Dell SonicWALL-Firewalls. Diese zeichnen sich durch dieselbe erstklassige Perimetersicherheit wie die anderen Firewalls der Produktpalette aus, sind jedoch auf eine größere Anzahl an Verbindungen und Benutzern und eine höhere Bandbreite ausgelegt. Durch die Integration mit Active Directory können Unternehmen granulare Kontrollen implementieren, sodass beispielsweise die Marketingabteilung Zugriff auf Social Media, jedoch keinen Zugang zu anderen, auf den entsprechenden Websites vorhandenen Services wie Spielen und Chats hat.

Wenn zwei oder mehrere Server vorhanden sind, auf denen dieselben Anwendungen ausgeführt werden, ist gegebenenfalls eine Lastverteilung erforderlich (bzw. vom Softwareanbieter vorgeschrieben), um die Clientverbindungen zwischen den Servern zu verteilen und im Falle eines Supplicant-Fehlers/Serverausfalls ein Failover zwischen den Servern zu ermöglichen. Der KEMP LoadMaster überzeugt durch eine robuste Konfiguration mit Standardfunktionen für Lastverteilung, Persistenz, erweiterte Integritätsprüfungen, Content Switching und Hochverfügbarkeit, auf deren Grundlage Administratoren extrem zuverlässige Netzwerke bereitstellen können.

Große Unternehmen habe typischerweise komplexere Anforderungen und benötigen dementsprechend auch komplexere Netzwerke. Dell SonicWALL und KEMP Technologies wachsen mit Ihrem Unternehmen – unabhänging davon, ob Sie Ihren Nutzern interne Anwendungen wie Exchange oder SharePoint oder öffentlich zugängliche Angebote wie Firmenwebsites und eCommerce zur Verfügung stellen.

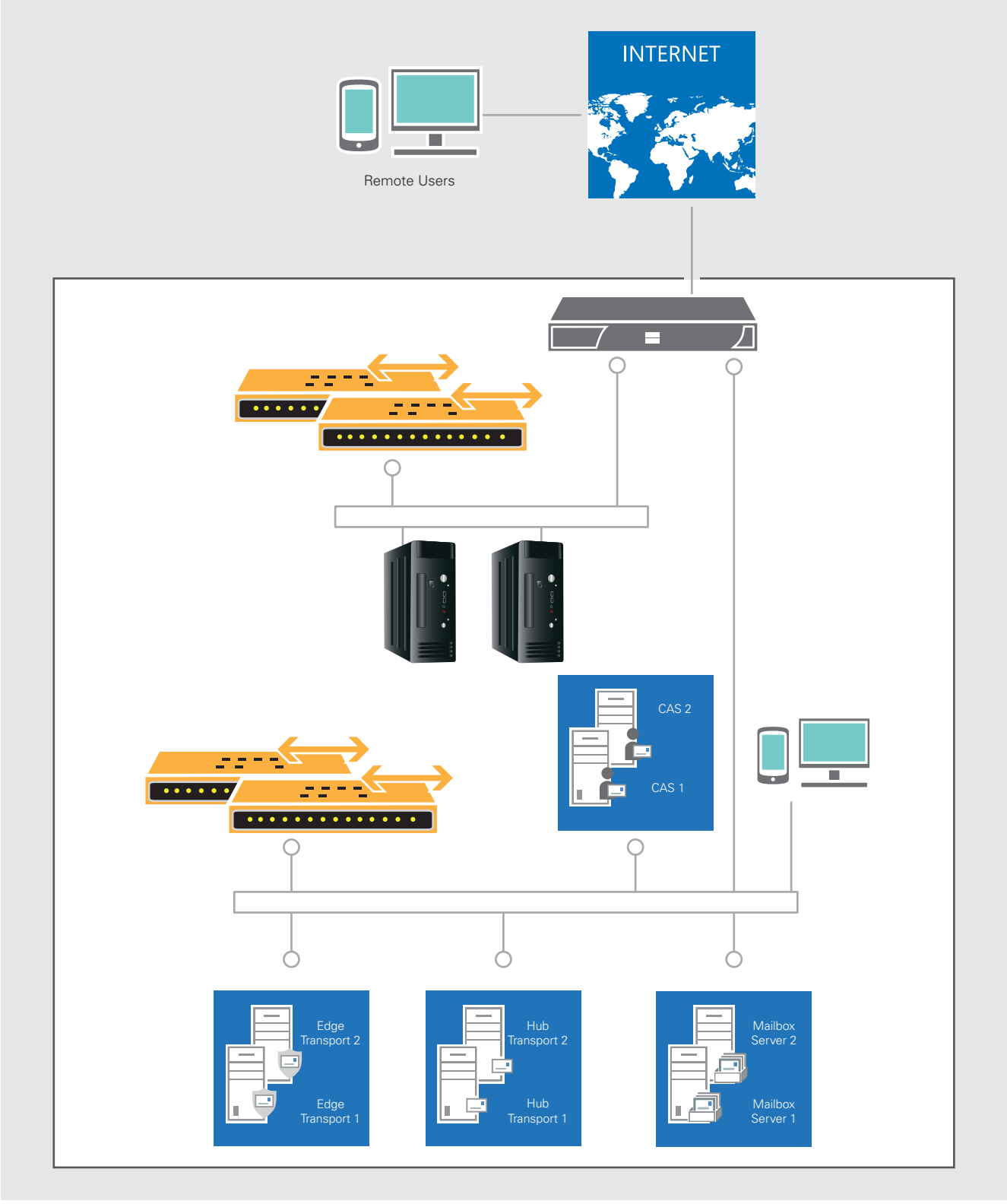
Netzwerke mit DMZ-basierten Services

In der letzten Beispielkonfiguration, Abbildung 4, werden öffentliche Services wie Unternehmenswebsites, eCommerce, Outlook Web Access, SharePoint etc. in einer DMZ implementiert. Andere Anwendungen und Services, wie Exchange, die ausschließlich zur internen Nutzung bestimmt sind, werden im LAN implementiert.

Dell SonicWALL-Firewalls lassen sich in Bezug auf die Performance und die Komplexität einer Implementierung skalieren. Hochverfügbarkeit und Clustering gewährleisten die Ausfallsicherheit in einem extrem wettbewerbsorientierten Geschäftsumfeld, bei dem der Verlust einer aufgabenkritischen Anwendung die Leistung und Rentabilität eines Unternehmens ernsthaft beeinträchtigen kann. Durch die Unterstützung mehrerer Sicherheitszonen (LAN, DMZ1, DMZ2, LAN2 usw.) und Implementierungsarten wie Layer 2-Bridge, geroutet oder NAT auf derselben Plattform kann ein Unternehmen Anwendungen und Services implementieren, ohne jegliche Kompromisse eingehen zu müssen. Dank der engen Integration mit Active Directory lassen sich Richtlinien wie Website- und Anwendungskontrolle, Firewall-Richtlinien, Bandbreitenmanagement etc. auf Benutzer-/Gruppenbasis ohne weitere Benutzerauthentifizierung anwenden (Single Sign-on).

Single Sign-on ist auch über die Integration mit RADIUS Accounting verfügbar. Auf diese Weise können Lösungen von Drittanbietern (z. B. Wireless LAN) den Benutzernamen/IP-Informationen an die Firewalls weiterleiten, sodass Sicherheitsrichtlinien basierend auf Benutzer-/Gruppeninformationen angewendet werden können. Auch in dermaßen komplexen Netzwerken zeichnen sich Dell SonicWALL Next Generation Firewalls durch herausragende Leistung und Sicherheit aus. Darüber hinaus können Deep Packet Inspection Services wie Intrusion Prevention, SSL-Inspektion, Gateway-Virenschutz und -Anti-Spyware ohne Beeinträchtigung der Anwendungsperformance genutzt werden.

Abbildung 4



Bei der Anwendungsveröffentlichung in diesen Umgebungsarten werden gegebenenfalls zwei oder mehr Load Balancer-Paare benötigt. Ein gutes Beispiel für dieses Szenario sind Umgebungen, in denen für Anwendungen in der DMZ (SQL/CRM und SharePoint) unterschiedliche Sicherheitsgrade für den Zugang externer Benutzer sowie Lastverteilungsanforderungen für mehrere Server bestehen.

Die Isolierung dieser Services verhindert unberechtigten Zugriff basierend auf der kollaborativen Sicherheit der DELL SonicWALL-Firewalls und auch Lastverteilungsfunktionen zur Gewährleistung der Ausfallsicherheit.

Wenn andere Services, wie z. B. Exchange, im LAN implementiert sind, ist die beste Vorgehensweise die Integration eines weiteren Load Balancer-Paars in der LAN-Sicherheitszone. In Topologien mit mehreren Zonen sind somit potenziell 4 oder mehr Load Balancer erforderlich. Alle KEMP LoadMaster-Produkte werden im Wesentlichen mit demselben Prozess implementiert, und die inhärenten Funktionen finden sich in der gesamten Produktpalette.

In Kombination mit den Produkten zur Lastverteilung können auch erweiterte Funktionen wie ESP (Edge Security Pack) und GSLB (Global Server Load Balancing) implementiert werden, wobei gegebenenfalls eine zusätzliche Lizenz benötigt wird. Diese Funktionen ermöglichen Single Sign-on, Vorautorisierung und globale (standortbasierte) Lastverteilung.

Die Next Generation Firewalls, Unified Threat Management (UTM)-Lösungen und SSL-VPNs von Dell SonicWALL übertreffen Microsoft Forefront TMG 2010 mit herausragenden Funktionen für Intrusion Prevention, Malware-Schutz, Application Intelligence und Anwendungskontrolle, Traffic-Visualisierung in Echtzeit, sicheren granularen Fernzugriff und Inspektion SSL-verschlüsselter Sessions.

Dell SonicWALL Next Generation Firewalls bieten Unternehmen jeder Größe erhöhte Netzwerksicherheit ohne Beeinträchtigung der Performance, da sie den gesamten Traffic unabhängig vom Port oder Protokoll überwachen, einschließlich des SSL-verschlüsselten Datenverkehrs. Diese kostengünstigen und einfach zu bedienenden Firewalls der nächsten Generation sind in der Lage, Verschleierungstechniken aufzuspüren und stellen netzwerkbasierte Anti-Malware mit Zugriff auf eine laufend aktualisierte Cloud-Datenbank bereit.

Die zentralisierten Verwaltungs- und Reporting-Funktionen des Dell SonicWall Global Management Systems gewährleisten eine einfache Bedienung, Überwachung und Bereitstellung verteilter Implementierungen. Über eine zentrale Managementoberfläche können einheitliche Sicherheitsrichtlinien für alle Geräte vorgegeben werden.

Die Dell SonicWALL Secure Remote Access (SRA)-Plattform und Appliance-Serie bietet eine sichere Komplettlösung für den gleichzeitigen Fernzugriff von bis zu 20.000 mobilen Unternehmensbenutzern über eine Einzelanwendung, ohne die Infrastrukturkosten oder die Komplexität zu erhöhen. Sowohl Mitarbeiter als auch Geschäftspartner im Extranet profitieren von einem sicheren, clientlosen Zugriff auf benötigte Ressourcen von nahezu jedem Gerät und jedem Ort aus und mit der einzigartigen Sicherheit von SSL-VPN.

Die Zuverlässigkeit eines Branchenführers

Dell SonicWALL kann auf über 20 Jahre Branchenerfahrung zurückblicken, und Dell wurde von Gartner als Branchenführer im Bereich der Netzwerksicherheitslösungen anerkannt. Im NGFW Product Analysis Report von NSS Labs im Jahr 2013 erhielt die SuperMassive Firewall von Dell eine Testbewertung von 100 Prozent in folgenden Bereichen: Anti-Evasion, Stabilität und Verlässlichkeit, Firewall, Anwendungskontrolle und Identitätsprüfungen.

Weitere Informationen zu den Dell SonicWALL-Netzwerksicherheitslösungen

Dell SonicWALL bietet eine umfassende Palette branchenführender Produkte für Netzwerksicherheit, darunter Next Generation Firewalls und Unified Threat Management (UTM)-Lösungen, sicheren Fernzugriff/SSL-VPN, Anti-Spam/E-Mail-Sicherheit, sowie zentralisierte Verwaltungs- und Reporting-Funktionen und technischen Support 24 Stunden pro Tag, 7 Tage die Woche.

Nützliche Online-Ressourcen:

- www.sonicwall.com
- www.livedemo.sonicwall.com
- http://www.demosondemand.com/clients/sonicwall/001/page/demos.asp
- Dell SonicWALL kontaktieren:
  http://www.sonicwall.com/us/en/company/286.html
- Microsoft Dell Global Alliance:
  http://www.microsoft.com/enterprise/partners/dell.aspx#fbid=PUqgSVat0g0

Die KEMP Technologies LoadMaster-Suite mit Application Delivery Controller-Lösungen optimiert die Web- und Anwendungsinfrastruktur, bietet Hochverfügbarkeit und flexible Skalierbarkeit und gewährleistet einen sicheren Geschäftsbetrieb bei gleichzeitigen Kosteneinsparungen im IT. Ergänzt durch das KEMP Edge Security Pack (ESP) stellt der LoadMaster eine Komplettlösung für Kunden bereit, die vormals TMG zur Veröffentlichung ihrer Microsoft-Anwendungen eingesetzt hätten.

Mit KEMP als Microsoft Gold Certified Partner im Bereich „Messaging und Kommunikation" können unsere Kunden sicher sein, dass sie die richtige Wahl getroffen haben, wenn sie KEMP-Produkte in ihr Netzwerk aufnehmen. KEMP bietet Unternehmen jeder Größe ein breites Angebot an virtuellen und Hardware-Produkten, die optimal auf die jeweiligen Netzwerk-, Größen- und Budgetanforderungen zugeschnitten sind.

Unabhängig von der Plattform stellen alle KEMP Load Balancer und ADCs folgende Funktionen bereit:

- Anwendungsintegritätsprüfung
- Content Switching
- Intrusion Prevention System
- Vorauthentifizierung
- Single Sign-on
- Content Caching
- Datenkomprimierung
- Layer 4-7-Server-Lastverteilung
- Serverintegritätsprüfung
- SSL-Offloading

Die KEMP Virtual LoadMaster-Produkte kombinieren diese Funktionsvielfalt mit einer benutzerfreundlichen Oberfläche und sind für die Hypervisoren VMware, Hyper-V, Xen, KVM und Oracle VirtualBox verfügbar. Die virtuellen Appliances sind für die Lastverteilung kleinster Anwendungen bis hin zu Großimplementierungen einsetzbar und erreichen einen Durchsatz von bis zu 5 Gbit/s und verarbeiten bis zu 10.000 SSL-Transaktionen pro Sekunde.

Sie können die KEMP Virtual Load Master herunterladen und 30 Tage unverbindlich testen. Eine kostenlose Testversion des VLM-5000 mit ESP- und GEO-Funktionalität finden Sie unter www.kemptechnologies.com/try.

Über KEMP Technologies

Mit über 16.000 Kunden weltweit und Niederlassungen in den USA, Europa, Asien und Südamerika ist KEMP Technologies seit 2000 ein führender Anbieter kosteneffektiver Load Balancer- und Application Delivery Controller-Lösungen, die sich durch ein erstklassiges Preis-/Leistungsverhältnis auszeichnen. Die flexible und leistungsstarke Architektur unserer Produkte garantiert höchste Wertschöpfung und ermöglicht unseren Kunden die Optimierung ihrer Geschäftstätigkeit und ihrer Interaktion mit Kunden, Mitarbeitern und Partnern auf der Grundlage einer internetbasierten Infrastruktur.

Über Dell Software

Dell Software hilft Kunden bei der besseren Nutzung ihres Potentials mit Hilfe von Technologie durch skalierbare, günstige und benutzerfreundliche Lösungen zur Vereinfachung der IT und zur Absicherung gegen Risiken. Das Softwareangebot von Dell richtet sich an fünf Schlüsselbereiche des Kundenbedarfs: Rechenzentrums- und Cloud-Management, Informationsmanagement, Mobile Workforce-Management sowie Sicherheit und Datenschutz. In Kombination mit Dell Hardware und Services bietet die Software unerreichte Effizienz und Produktivität zur Beschleunigung der Unternehmensergebnisse.

Über ADN

ADN vertreibt als Value-Added IT-Distributor herstellerübergreifende End-to-End-Lösungen und Produkte aus den Bereichen Server & Storage, Virtualisierung & Cloud, Unified Communications & Mobility, Networking & Security sowie Big Data & Business Intelligence an IT-Wiederverkäufer. Zu den zusätzlichen Services zählen u. a. Herstellertrainings sowie Beratung und Support im gesamten Projektablauf.

Für weitere Informationen stehen Ihnen Ihre persönlichen Ansprechpartner von ADN gerne persönlich zur Verfügung:

Marcel Horion
Business Development Manager
Dell SonicWALL

Tel.: +49 2327 9912-206
E-Mail: marcel.horion@adn.de

Johannes Dahmen
Business Development Manager
KEMP Technologies

Tel.: +49 2327 9912-271
E-Mail: johannes.dahmen@adn.de

ADN® Advanced Digital
Network Distribution GmbH

Josef-Haumann-Str. 10 | 44866 Bochum
Tel.: +49 2327 9912-0 | E-Mail: info@adn.de | Web: www.adn.de