Purview™ – Netzwerkbasierte Applikationsanalytik und -optimierung

WHITE PAPER

Purview

Technische Übersicht

Übersicht

Extreme Networks Purview ist eine netzwerkbasierte Applikationsanalyse- und Optimierungslösung, die Anwendungsdaten sammelt und analysiert, um Informationen über laufende Applikationen, Nutzerverhalten, räumliche Verteilung der Daten und im Netzwerk aktive Geräte darzustellen. Purview nutzt die patentierte Coreflow2™ ASIC Technologie von Extreme, macht dadurch die Nutzung von Applikationen in Netzwerken sichtbar und hilft Unternehmen damit gleich in vierfacher Hinsicht: Qualitätssteigerung für Anwender, die Applikationen und Services im Netzwerk nutzen; Verstehen von Nutzerverhalten; Verbesserung der Applikations-Performance; Schutz gegen den nicht autorisierten oder schadhaften Einsatz von Applikationen.

Mithilfe von Purview können IT-Abteilungen nun signifikante Verbesserungen bei den unternehmenskritischen technologischen Anwendungen erzielen.

In der heutigen hochvernetzten und reizüberfluteten Welt wird es immer schwieriger, Nutzerverhalten zu erfassen, das Nutzererlebnis im Bereich mobiler Kommunikation sowie Social Media zu verbessern und dabei die Zuverlässigkeit des unternehmenskritischen Netzwerks zu gewährleisten. Purview löst diese komplexen Anforderungen durch die Integration von Netzwerkdaten, die einen Kontext zwischen Nutzern, Geräten, Standorten und verwendeten Applikationen herstellen. Netzwerkdaten werden erfasst und anschließend kumuliert, analysiert, gekennzeichnet und korreliert, um dann entsprechende Reports zu liefern. Purview schließt damit die Lücke zwischen Netzwerk-Management, Security und Business Analytics durch eine einheitliche, integrierte Sichtweise. Das hilft Unternehmen dabei, die Qualität für Anwender zu steigern, den wachsenden Anforderungen von Nutzern zu entsprechen und die Applikations-Performance zu steigern. Purview kann in bestehenden oder neuen Netzwerken mit Switches von Extreme Networks oder jedem anderen Anbieter eingesetzt werden. Purview kann Applikationsdaten über das gesamte Netzwerk hinweg sammeln, analysieren und optimieren. Dies beinhaltet Daten aus kabellosen und –gebunden Netzen sowie aus Core und Data Center.

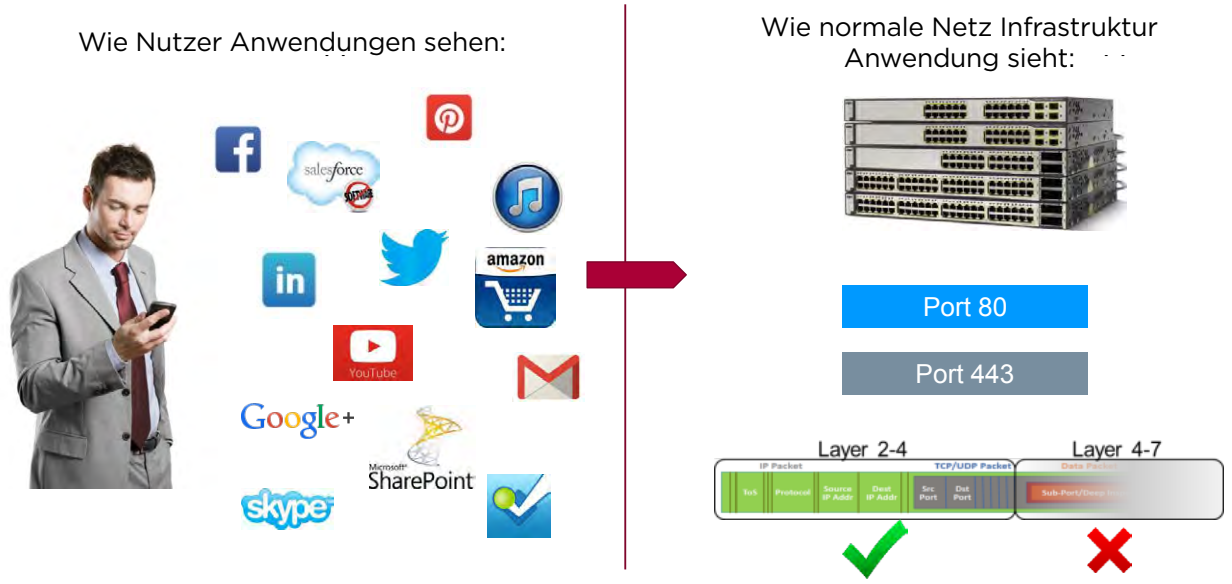


Abb. 1: Keine Visibilität und Kontrolle über Applikationen

Vorteile der Lösung im Überblick

- Business Analytics – Analyse der Nutzung von Applikationen und deren Reaktionszeiten.
- IT-Netzwerk-Management – Schnellere Problemlösung durch Erfassen der Applikations- und Netzwerk-Performance sowie Optimierung des Netzwerkdesigns für ein verbessertes Nutzererlebnis.
- Netzwerksicherheit – Identifizierung von nicht autorisierten und schadhaften Applikationen zur Einhaltung von Compliance-Richtlinien.
- In Verbindung mit der Network Access Control (NAC) Lösung von Extreme Networks steigert Purview die Effizienz der IT durch noch umfassendere Analysefunktionen, die Benutzernamen, Standort, Gerätetyp, Netzwerkrichtlinien und vieles mehr beinhalten.
- Purview basiert auf der patentierten CoreFlow2™ ASIC Technologie, die den Zugriff auf Anwendungsnutzungsdaten während ihrer Übertragung im Netzwerk ermöglicht.
- Bereits bei der Einführung unterstützt Purview über 13.000 Applikations-Profile. Dazu gehören die Bereiche Enterprise CRM, ERP, HCM, Storage, Internet, Collaboration, Email, Soziale Netzwerke und Gaming.

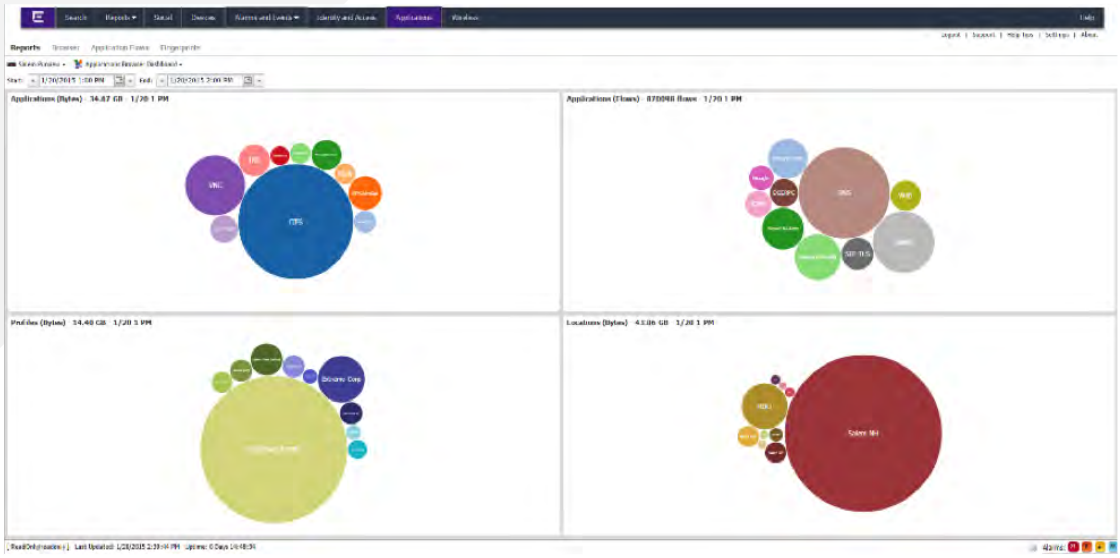


Abb. 2: Dashboard

Architektur

Die Purview Lösung ist aus vier Elementen aufgebaut

- Die Purview Engine, die sowohl als virtuelle Maschine für VMware oder als Hardware Appliance zur Verfügung steht.
- Netsight Management
- Eine Netzwerk-Infrastruktur, die unsampled Netflow Daten und Traffic Mirror Funktionalität in Echtzeit liefert.
- Die notwendigen Lizenzen um die einzelnen Elemente zu betreiben (Netsight, Flow-Lizenzen, usw.)

Die Purview Engine empfängt Netflow Records und einen korrespondierenden Daten Satz aus dem Traffic Mirror für die Analyse. Mit beiden Informationssätzen korreliert die Purview Engine die Netflow Statistiken, die ihr die Informationen über Teilnehmer des Daten-Flows und über Menge

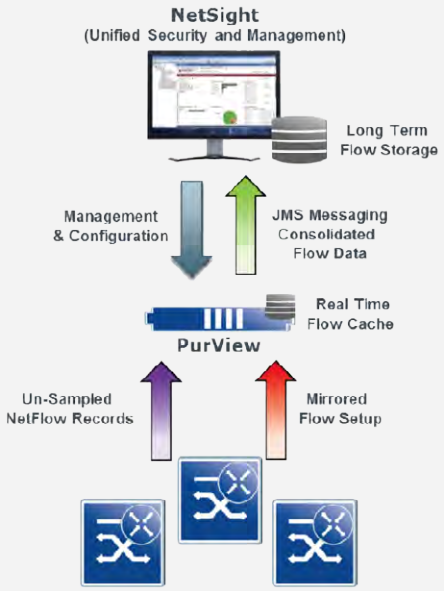


Abb. 3: Netzwerkinfrastruktur

und Art der Daten liefern mit den Applikations-Informationen, die ihr über den korrespondierten Datensatz zur Verfügung gestellt werden. Diese Daten werden zusammengefasst und der Management-Lösung Netsight für graphische Darstellung und Speicherung der Informationen übergeben.

Durch den Einsatz der einzigartigen Coreflow2 Architektur von Extreme (S-, K-Serie und Purview Flow Collector) ist Purview eine Lösung für Netzwerk-Infrastrukturen mit hoher Datendurchsatz-Rate im Core und Data Center Bereich, in dem sowohl die Verarbeitung von Daten aus einer Multi-Gigabit Umgebung - ohne Einsatz von kostenintensiverer Hardware – ermöglicht wird, als auch eine Entkopplung von Switch und Application Intelligence ermöglicht wird. Die Coreflow2 Technologie liefert drei nötige Funktionen:

- **Unsampled Netflow** – Die CoreFlow2 Architektur erlaubt die Lieferung von unsampled Netflow Daten, unabhängig von Anzahl und Bandbreite der Datenschnittstelle und ohne Beeinträchtigung der Switch Performance des Systems. Dadurch ist eine akkurate statistische Erfassung der Verkehrsbeziehungen möglich
- **MirrorN Feature** – Das MirrorN Feature in Extreme-Geräten mit CoreFlow2 Technologie ermöglicht es, eine Policy zu erstellen, die nur die ersten 15-30 (N) Pakete einer Datenverbindung (Flow) auf einen Mirror Port spiegelt. Über diese Policy werden nur die notwendigen Informationen über eine Datenverbindung an die Purview Engine gesendet. Dadurch wird die Menge der zu analysierenden Daten auf die relevanten Informationen zur Applikationsidentifizierung eingegrenzt.
- **Remote Mirroring über GRE L2 Tunneling** – Über Remote Mirroring kann eine einzelne Purview Engine die Daten von mehreren Switchen oder Purview Flow Collectoren bearbeiten, ohne direkt mit Ihnen verbunden zu sein.

Abb. 4: Aufbau und Bestandteile der Purview Lösung

Purview hilft der IT Administration, Entscheidungen zu treffen und gibt Ihnen hilfreiche Informationen zu Situationen, denen Sie in ihrer täglichen Arbeit gegenüber stehen. Im Folgenden ein paar Beispiele, wie Purview genutzt werden kann, um häufige Probleme in Netzwerken zu lösen.

Data Center Performance Analyse

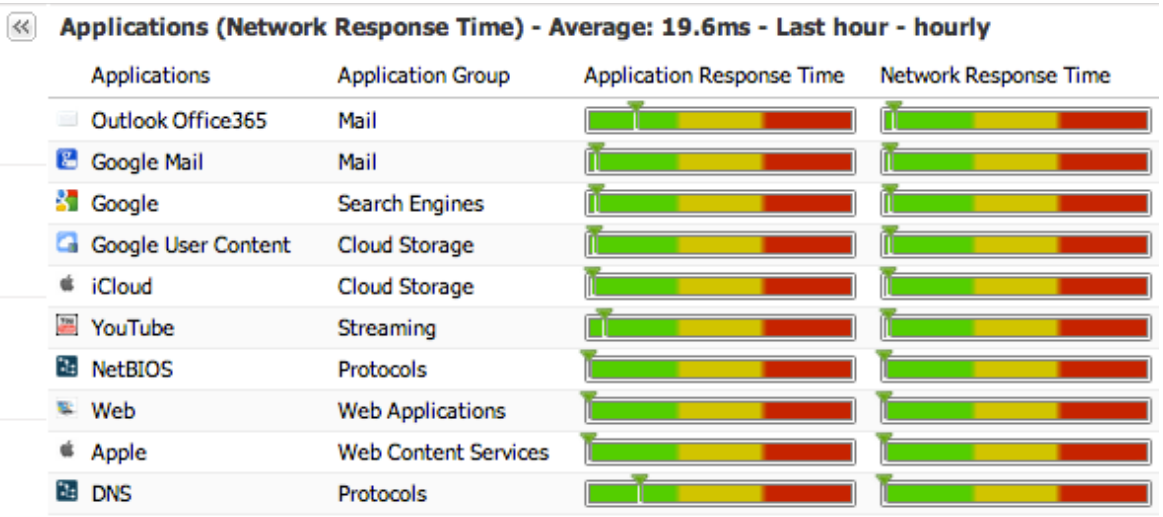
Um die optimale Auslastung der vorhandenen Netzwerk-Ressourcen zu erreichen, ist es oft sinnvoll, Anwendungen an unterschiedliche physikalische Lokationen zu verteilen. Aus Gründen der Performance oder aus Wartungsgründen müssen virtuelle Applikationsserver im Netzwerk verschoben werden. Vor diesen Aktionen ist es sinnvoll und notwendig festzustellen, wie die Anwendungen von End Usern genutzt werden und in welchen räumlichen Lokationen wie viele User auf die Anwendungen zugreifen. Zusätzlich ist es wichtig zu wissen, in welchem Zeitraum die wenigsten User auf dieser Anwendung arbeiten, um den Termin des Umzugs oder der Wartung festzulegen.

Purview bietet hier die Möglichkeit, den Datenverkehr auf räumliche Verteilung und Nutzerverhalten zu analysieren und über die OneView Oberfläche von Netsight darzustellen. Anhand der Informationen aus den einfach verständlichen Graphen lässt sich ablesen, zu welcher Zeit ein Umzug der Anwendung am wenigsten Nutzer betrifft und wo der beste Standort für die Anwendung ist.

Abb. 5: Darstellung von User pro Zeit und Applikation

Application-Response vs. Network-Response

Die meisten Fehlermeldungen von Endanwendern sind in ihren Aussagen zu diffus, um eine schnelle Problemanalyse zu ermöglichen. Eine Aussage wie „Das Netzwerk ist langsam“ lässt keine Rückschlüsse darauf zu, wo die tatsächliche Störung des Datenverkehrs zu finden ist. Für den Administrator ist es oft schwer heraus zu finden, ob das Problem am Endgerät/dem Nutzer, der Netzwerk-Infrastruktur oder der Anwendung liegt, die der End User benutzen möchte.



Applications (Network Response Time) - Average: 19.6ms - Last hour - hourly

Applications	Application Group	Application Response Time	Network Response Time
Outlook Office365	Mail		
Google Mail	Mail		
Google	Search Engines		
Google User Content	Cloud Storage		
iCloud	Cloud Storage		
YouTube	Streaming		
NetBIOS	Protocols		
Web	Web Applications		
Apple	Web Content Services		
DNS	Protocols		

Abb. 6: Reaktionszeit der Applikationen vs. Netzwerk

Purview bietet hier im Zusammenspiel mit NAC eine Anzahl von Informationen, die eine Eingrenzung und Lösung des Nutzerproblems beschleunigen und ermöglichen. Purview kann bis auf das Nutzer-Level die Antwortzeiten einzelner Anwendungen sowohl auf Netzwerkebene, als auch auf Anwendungsebene darstellen. Es können z. B. Analysen über Netzwerk-Antwortzeiten in Relation zu Anwendungs-Antwortzeiten durchgeführt werden. Dies kann auf einer zeitlichen Basis oder auf den Nutzer spezifisch dargestellt werden.

Erkennung von schädlichen Applikationen

Neue Sicherheitsbestimmungen verlangen von einem Administrator immer umfangreichere Maßnahmen, um Anwendungen zu sperren oder den Gebrauch von nicht erlaubten Anwendungen zu erkennen. Purview ermöglicht es zu analysieren, welche Anwendungen im Netzwerk aktiv sind und gegebenenfalls von welcher Nutzergruppe diese Anwendungen eingesetzt werden. Werden Applikationen benutzt, die für spezifische Bereiche/Usergruppen nicht freigegeben sind? Sind nicht erlaubte Anwendungen im Netzwerk aktiv?

Überwachung von Anwendungs Roll-Out und Nutzung von lizensierten Anwendungen

Purview ist ein nützliches Hilfsmittel, um heraus zu finden, wie eine neue Anwendung vom Nutzer angenommen wird. Bei vielen IT-Abteilungen geht man davon aus, das ein Software Projekt abgeschlossen ist, wenn man die Anwendung jedem Nutzer zur Verfügung gestellt hat. Ob die neue Anwendung wirklich vom Endnutzer angenommen, kann nicht überprüft werden. Hier hilft Purview. Man kann sehr einfach darstellen, wie viele Nutzer, wie häufig eine Anwendung nutzen und von welchen Arbeitsgruppen/Lokationen auf diese Anwendung zugegriffen wird.

Application/Client (Flows) - 148357 flows - Last hour

Application	Client	Application Group	Flows	Outbound Flows	Inbound
ClearCase	[redacted]-ws1.corp.extr...	Business Applications	51893	25942	25951
Encrypted Web	134.141.[redacted]	Web Applications	24208	12204	12004
Extreme Networks	134.141.[redacted]	Corporate Website	14255	14255	0
Microsoft SQL Server	[redacted]p-ws.corp.extr...	Databases	8574	4287	4287
Microsoft SQL Server	[redacted]r-ws.corp.extr...	Databases	8521	4321	4200
LDAP	134.141.[redacted]	Protocols	8330	4168	4162
Microsoft SQL Server	[redacted]mo-pc.corp.ex...	Databases	8264	4132	4132
Microsoft SQL Server	[redacted]-ws1.corp.extre...	Databases	8146	4073	4073
Microsoft SQL Server	[redacted]-ws1.corp.e...	Databases	8132	4066	4066
nmcdns175	[redacted]ay.ets.ente...	Web Applications	8034	4020	4014

Abb. 7: Flows pro Applikation/Client

Zusammenfassung

- Intuitive Dashboards und Reporting
  - Überblick aller Applikationen, Bandbreitennutzung, Clients, Flows sowie Performance des Netzwerks und der Applikationen
  - Spezifische Dashboards
- Durchgängige Beobachtung von Applikationen im gesamten Netzwerk
  - Von Edge über Data Center und Core zum Internet
- Offene & anpassbare Applikationsdaten und -profile
  - Akkurat durch Signaturen & Heuristik
  - Mehr als 13,000 Daten für mehr als 7,000 Applikationen sofort verfügbar
  - Hinzufügen von eigenen Applikationsprofilen möglich
- Detaillierte Informationen über Nutzung und Performance von Applikationen
  - pro Applikation, User, Gerätetyp, Ort, etc.
- Kontextuelle Information der Applikationen
  - Nutzer, Profil, Ort, Zeit, Gerät & mehr
- Applikation und Netzwerk Performance Tracking
- Netzwerkübergreifend
- Decodierung von Applikation – unabhängig vom Port
- Eine einzige Architektur für Access, Distribution, Core, Data Center, übergreifend
- Tbit/s Geschwindigkeiten und Skalierung bis zu Millionen von Flows ohne die Switch-Performance zu beeinträchtigen

Extreme networks

http://www.extremenetworks.com/contact / Phone +1-408-579-2800

©2015 Extreme Networks, Inc. All rights reserved. Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries. All other names are the property of their respective owners. For additional information on Extreme Networks Trademarks please see http://www.extremenetworks.com/company/legal/trademarks. Specifications and product availability are subject to change without notice. 9780-0615-25