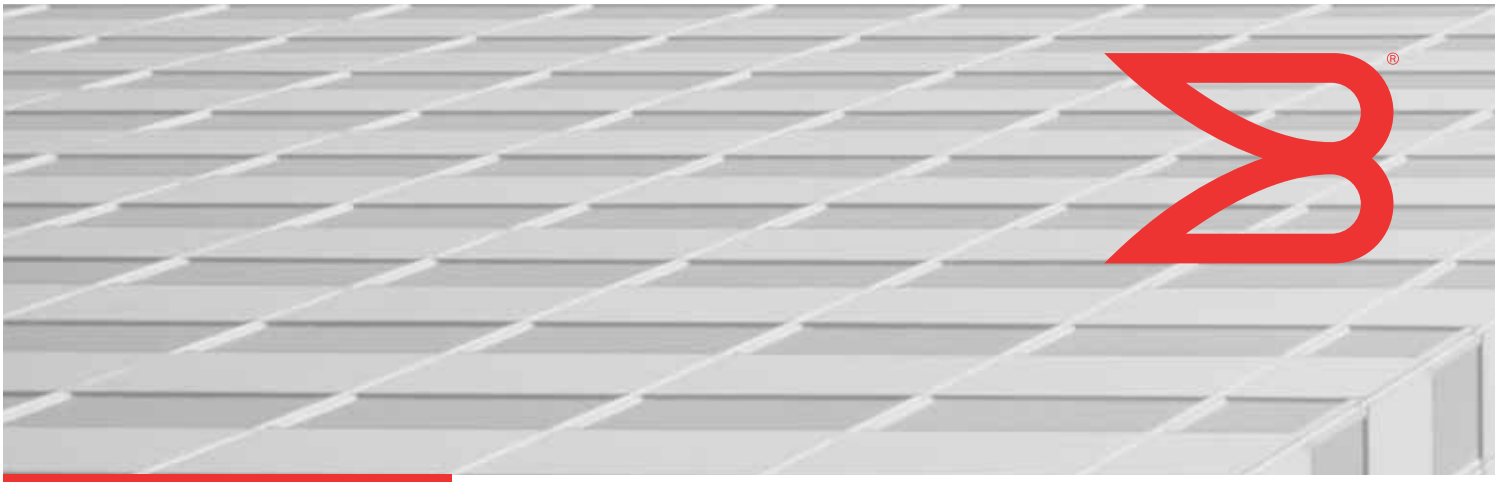

CAMPUS-NETZWERK

Software-Defined Networking im Campus-Netzwerk

Dynamische Orchestrierung und Bereitstellung von Ressourcen im Campus-Netzwerk mittels Software-Defined Networking (SDN).

BROCADE

Schon seit Jahren sind zentralisierte Anwendungen für die Überwachung der ordnungsgemäßen Funktion von Netzwerken auf dem Markt. Bei diesen Anwendungen werden verschiedene Mechanismen für die Steuerung von Netzwerk-Geräten „zusammengeflickt“. Für jeden Netzwerk-Anbieter brauchten diese Anwendungen ein spezielles Plugin, und – in manchen Fällen – wurden sogar mehrere Plugins für einen Anbieter benötigt, weil es innerhalb der Produktlinien des Anbieters große Unterschiede gab. Üblicherweise brachten neue Software-Releases eines Netzwerk-Anbieters die Anwendung zum Absturz und erforderten wiederum Updates in der Anwendung. Aufgrund der hohen Kosten für Entwicklung und Wartung waren diese Anwendungen sehr teuer in der Anschaffung.

Software-Defined Networking (SDN) löst dieses Problem, indem Schnittstellen zwischen dem zentralisierten Controller und den Netzwerk-Geräten definiert werden. Diese Schnittstellen bleiben unabhängig von beliebigen Software-Änderungen auf beiden Seiten transparent, solange die Updates genau der definierten Schnittstellendefinition entsprechen. Damit ist eine schnellere Entwicklung zuverlässiger, langlebiger Anwendungen möglich, die unabhängig von den Geräten im Netzwerk sind. Daraus entsteht eine neue Reihe kostengünstiger SDN-Anwendungen, mit denen Netzwerk-Ressourcen exakt auf die Anforderungen der Anwender und ihrer Anwendungen im 21sten Jahrhundert abgestimmt werden können.

CAMPUS-NETZWERKE IM 21STEN JAHRHUNDERT

Der Informationsfluss im Campus-Netzwerk ist die Lebensader eines Unternehmens. Die Informationen müssen ungestört fließen und gleichzeitig kontrolliert und überwacht werden, um die Sicherheit und Integrität zu gewährleisten. Die Anwendungen haben sich weiterentwickelt – von Email, Drucken und Datei-Übertragungen hin zu zeitkritischen Video- und Audio-Übertragungen, Real-Time Imaging und riesigen Big-Data-Übertragungen.

Herkömmliche Architekturen und Netzwerk-Protokolle versuchen, den Anforderungen nach Agilität und Flexibilität gerecht zu werden, und befinden sich dabei bereits jetzt an der Grenze der Belastbarkeit. Um den sicheren und freien Fluss der Informationen im Campus sicherzustellen, sind neue Architekturen und Protokolle erforderlich.

Die Brocade® HyperEdge® Architektur ermöglicht eine neue Netzwerk-Topologie, um den physischen Anforderungen für die Datenübertragung gerecht zu werden. SDN ist zu einer der Schlüssel-Technologien der HyperEdge-Architektur geworden. OpenFlow läuft auf Brocade Switches und kann entweder den gesamten Datenverkehr auf einem bestimmten Link beeinflussen oder zusammen mit herkömmlichen Protokollen operieren, die den Hybrid Per-Flow-Modus von Brocade nutzen. Damit ist es möglich, bestimmte Datenflüsse auf einem Link zu manipulieren; gleichzeitig kann es anderen Datenflüssen gestattet werden, die übliche Paketverarbeitungs-Pipeline zu nutzen.

Dank SDN können Sie den Datenverkehr im Netzwerk maßgeschneidert lenken. Die SDN-Anwendung akzeptiert Input aus zahlreichen Quellen: Statistiken zu physischen Netzwerk-Daten, Login- und Logoff-Informationen der Anwender im Netzwerk, Start- und Stopp-Informationen zu hoch priorisierten Benutzer-Anwendungen, auf Basis historischer Trends berechneter voraussichtlicher Datenverkehr, Analysen zu Sicherheitsbedrohungen, und so weiter. Diese Informationen können dann als Entscheidungsbasis für die jeweiligen Reaktionen verwendet werden. Der SDN-Controller entscheidet dann – basierend auf der von ihm erstellten Netzwerkkarte – wo Änderungen im Netzwerk vorgenommen werden. Dabei kann es sich um etwas Einfaches wie die Erhöhung der Priorität des Datenflusses einer bestimmten Anwendung handeln – bis hin zu einem kompletten Zugriffskontroll-System für das Netzwerk inklusive Rollen-basierter Ressourcenzuweisung. All diese Komponenten operieren unabhängig voneinander auf unterschiedlichen Layers, mit einem festgelegten API zwischen den jeweiligen Layers und einem vordefinierten Messaging Set. Dies ermöglicht einen stabilen Funktionsumfang, der je nach den Möglichkeiten, die sich die Layer untereinander mitteilen, skaliert wird. Im Gegensatz zum bisherigen Ansatz verursacht ein Update in einem Layer keine Unterbrechung in der Funktionalität eines anderen Layers.

Brocade hat sich für eine Standardisierung auf OpenFlow Version 1.3 – inklusive den im Vergleich zu Version 1.0 entsprechend verbesserten Möglichkeiten in den Bereichen Funktionalität, Hochverfügbarkeit und Sicherheit – und somit für eine stabileEnterprise-Lösung entschieden. Einige Anbieter haben sich dafür entschieden, OpenFlow mit CPU-gebundener Software-Verarbeitung und Weiterleitung des Datenflusses zu implementieren. Um den höchstmöglichen Performance-Level zu gewährleisten, implementiert Brocade die Verarbeitung des Datenflusses ausschließlich auf Hardware-Basis.

Der Revisions-Stand von OpenFlow (Version 1.3.00 vs. 1.0.00) definiert den vollständigen Satz an Fähigkeiten, den jede Komponente (Anwendung, Controller und Switch) theoretisch unterstützen kann. Die im OpenFlow integrierte automatische „Capability of Discovery“ ermöglicht eine „scheibchenweise“ Aufrüstung jeder einzelnen Komponente, ohne die Kompatibilität zu verletzen. Dadurch kann jedes Gerät von Brocade – egal ob Brocade ICX® Series Switch, Brocade MLXe® Series Router, oder ein Brocade VDX® Series Switch – mit jedem SDN-Controller zusammenarbeiten, auf dem die gleiche OpenFlow-Version läuft. Da die von dieser speziellen OpenFlow-Version unterstützte Funktionalität auf den jeweiligen Geräten aktiviert wird, integriert sich die neue Funktionalität nahtlos mit dem SDN-Controller und den oberhalb des Controllers laufenden Anwendungen.

Auf Basis der Erfahrungen in der Praxis hat Brocade die Implementierung von OpenFlow mit dem Hybrid Per-Flow-Modus weiterentwickelt und verbessert. Damit können Sie OpenFlow- und standardmäßige Paketverarbeitungs-Pipelines mischen – nicht nur auf Per-Port-Basis, sondern auch auf Per-Flow-Basis. Damit ist die Lösung von Brocade in der Lage, im Campus-Netzwerk die Leistungsfähigkeit von SDN für spezielle Benutzer- oder Anwendungs-Datenflüsse freizuschalten, während gleichzeitig für das Switching und Routing des verbleibenden Datenverkehrs im Netzwerk die standardmäßigen Paketverarbeitungs-Pipelines verwendet werden. Diese Hybrid-Modus-Fähigkeit von OpenFlow steht auf den Brocade ICX Switches im Access und Aggregation Layer, auf dem Brocade MLXe Router für den Core, und auf dem Brocade VDX Switch für die Brocade VCS® Fabric im Rechenzentrum (basierend auf der Brocade VCS Fabric-Technologie) zur Verfügung; all diese Komponenten arbeiten zusammen und bieten damit eine umfassende SDN-Lösung.

In den folgenden Abschnitten dieses White Papers werden eine Reihe möglicher Use Cases für SDN im Campus-Netzwerk beschrieben. Dabei handelt es sich nicht um eine umfassende Liste aller denkbaren Einsatzmöglichkeiten, sondern lediglich um einen Überblick über die Chancen, die SDN im Campus-Netzwerk eröffnet. Die beschriebenen SDN-Anwendungen sind derzeit möglicherweise noch nicht verfügbar bzw. befinden sich noch in der Entwicklungsphase und werden nicht unbedingt von Brocade, sondern von anderen Herstellern bereitgestellt.

Anwendungs-basierte Ressourcenzuteilung

Eine Anwendung konnte traditionellerweise einfach anhand der IP Port-Nummer in einem Packet Header identifiziert werden. Diese Nummern konnten statisch konfiguriert werden; dabei konnte dem Netzwerk-Verkehr einer ausgewählten Gruppe von Anwendungen eine höhere Priorität gegenüber anderen Anwendungen eingeräumt werden. Ein VoIP-Telefon (Voice over IP) beispielsweise generiert SIP-Verkehr (Session Initiation Protocol), und diesem SIP-Verkehr konnte im gesamten Netzwerk hohe Priorität eingeräumt werden.

Immer häufiger gehen Netzwerk-Administratoren den Weg von einer Reihe vernetzter Geräte auf dem Schreibtisch hin zu einem einzigen Gerät: in erster Linie ein Laptop, eventuell noch ein Tablet mit Docking Station oder ein Softphone. Gleichzeitig bewegen sich immer mehr Anwendungen von dedizierten Apps hin zur Integration in HTML und nutzen dabei HTTP als bevorzugtes Transportmittel. Zusammengenommen machen diese beiden Trends das bisherige Verfahren mit statischen ACL-Einträgen (Access Control List) unbrauchbar. Die Information zum IP-Port eines Pakets ist für Datenverkehr mit niedriger und hoher Priorität identisch und im HTTP-Verkehr über Port 80 verborgen. Die MAC-Adresse der Quellen sind ebenfalls identisch, da es keine Möglichkeit gibt, ein VoIP-Telefon von einem Laptop zu unterscheiden; daher erscheinen der Verkehr eines Softphones und das Surfen im Web gleich zu sein. In diese Fall besteht eine Option darin, dem ToS- (Type of Service) und DSCP-Wert (Differentiated Services Code Point) des Pakets zu vertrauen. Dabei wird jedoch angenommen, dass die Anwendungen auf dem Gerät zuverlässig die korrekten Werte anwenden; dadurch könnte aber ein Malware-Programm ein Netzwerk mit fingiertem hochprioritären Datenverkehr überschwemmen. Um festzustellen welche speziellen Datenflüsse mit hoher Priorität behandelt werden sollen, ist also ein neuer Mechanismus erforderlich, der alle anderen Datenflüsse standardmäßig auf niedrige Priorität setzt. Der Einsatz von SDN mit hybriden Ports auf dem Access Switch kann dieses Problem lösen.

Lassen Sie uns dies am Beispiel von Microsoft Lync untersuchen. Der Prozess, der bei einem Anruf in Gang gesetzt wird, sieht vereinfacht so aus: Ein Anwender mit einem an einen Laptop angeschlossenen Headphone startet Lync mit Web-Interface und ruft einen Kollegen aus der Kontaktliste an. Der Controller des Lync-Anrufs wandelt diese Kontaktinformation in eine IP-Adresse um und sendet diese IP-Adresse dann zum Lync-Client, der auf dem Laptop läuft. Ein Gespräch zwischen der IP-Adresse des Kontakts und der IP-Adresse des Laptops beginnt. Das Paket enthält jedoch keinerlei Informationen dazu, dass es höhere Priorität haben sollte als anderer Datenverkehr. Und an dieser Stelle kommt SDN ins Spiel.

Wenn der Controller des Lync-Anrufs die IP-Adresse zum Lync-Client auf dem Laptop sendet, kann er in einer SDN-Umgebung auch so konfiguriert werden, dass er diese Information auch an eine SDN-Anwendung sendet; deren Funktion wiederum liegt darin, mit einem SDN-Controller zu kommunizieren und für bestimmte IP-Paare in einem Netzwerk die jeweiligen Prioritäten festzulegen. Ein Lync-Anruf zum Beispiel könnte damit auf eine hohe Priorität gesetzt werden. Die SDN-Anwendung teilt dem SDN-Controller mit, dass die Priorität für ein bestimmtes IP-Paar auf „hoch“ gesetzt werden und der Verkehr über nicht überlastete Links geführt werden soll.

Der SDN-Controller nimmt diese Information entgegen und legt – basierend auf der Topologie, die er aus den Informationen erstellt hat, die er von allen OpenFlow-fähigen Geräten im Netzwerk erhalten hat – den optimalen OpenFlow-Pfad fest. Dieser Pfad beginnt an der Stelle, an der das Paket das Netzwerk betreten hat, und endet an der Stelle, an der es das Netzwerk verlässt (in beiden Richtungen); damit ist der optimale Pfad für die den Fluss der Anrufpakete durch das Netzwerk festgelegt. Dazu gehört möglicherweise auch, dass Pakete über andere Links als bei der herkömmlichen Pipeline geführt werden. Diese Informationen zum angepassten Datenfluss werden – zusammen mit den dafür notwendigen Aktionen – an jeden der OpenFlow-fähigen Switches weitergegeben („Push“). Falls der Anruf innerhalb derselben Organisation stattfindet, befinden sich diese Einträge auf dem Brocade ICX 6610 Access Switch, mit dem beide Anwender verbunden sind, sowie auf den ebenfalls beteiligten Brocade ICX 6610 und Brocade MLXe Geräten im Netzwerk. Wird der Anruf beendet, „veralten“ die OpenFlow-Einträge wegen Inaktivität; damit werden die Ressourcen wieder für andere Anrufe oder hochprioritären Datenverkehr freigegeben.

Eine interessante Verbesserung in diesem Bereich überwacht den Datenverkehr einiger Anwendungen, wohingegen andere – in diesem Fall VoIP-Anrufe – nicht berücksichtigt werden. Zusätzlich zum Lync Call Manager, der die Flussinformationen an die SDN-Anwendung sendet, könnte eine zweite Quelle eine Liste von Quell- und Ziel-IP-Paaren senden, die überwacht werden sollen. Sobald die Lync-Information empfangen wird, wird der priorisierte Pfad durch das Netzwerk festgelegt (falls das IP-Paar auf der Watch List aufgeführt ist). Zusätzlich dazu kann – neben der „Set Priority“-Aktion – eine „Copy Packet“-Aktion hinzugefügt werden; damit wird eine Kopie des Anrufs an eine Sicherheits-Instanz gesendet. Dabei ist es nicht erforderlich zu wissen, wie die Mirroring-Funktion auf einem Switch funktioniert; es müssen auch nicht mehr Informationen als notwendig gesammelt werden. Sie verwenden einfach das OpenFlow-Protokoll, um die Aufgabe zu implementieren.

Diese neue SDN-Funktion nutzt das Wissen über den Datenfluss-Setup mit Hilfe von Anwendungen, die im Hintergrund ablaufen. Diese liefern die Informationen, die für die Identifizierung der Datenflüsse notwendig sind, die priorisiert oder auf dem Weg durch das Netzwerk mit zusätzlicher Bandbreite versorgt werden müssen. Solange alle Layers mit derselben OpenFlow-Version arbeiten, müssen für leistungssteigernde Geräte im Netzwerk keine Anwendungen umgeschrieben werden.

Rollen-basierte Ressourcenzuteilung

Es ist häufig sinnvoll, für Anwender – basierend auf ihrer Rolle innerhalb einer Organisation – festzulegen, was diese innerhalb des Netzwerk tun können bzw. nicht tun dürfen. Für diese Art der Konfiguration können Sie das IEEE 802.1X Protokoll nutzen. Der Access Switch agiert als „Authenticator“, der die Information an einen RADIUS-Server (Remote Authentication Dial-In User Service) leitet. Der RADIUS-Server wiederum beglaubigt den Benutzernamen und das gesendete Passwort. Falls dem Benutzer der Zugriff gewährt wird, sendet der RADIUS-Server diese Information an den Switch, der dem Benutzer Ressourcen zuweisen soll, und verwendet dabei VSA-Felder (Vendor Specific Attribute) in der RADIUS-Antwort. Damit wird die übergeordnete Authentication-Anwendung (der RADIUS-Server) eng mit dem Gerät auf dem Netzwerk-Layer verknüpft. Wenn sich die Fähigkeiten des Access-Gerätes ändern, muss der Zugang zum RADIUS-Server aktualisiert werden. Andernfalls kann es vorkommen, das Endanwender nicht authentifiziert werden. Oder noch schlimmer: Anwender werden authentifiziert, aber die für diese Anwender gültigen Sicherheits-Einschränkungen werden nicht mitgeliefert. Dies gilt insbesondere für alle NAC-Tools (Network Access Control), bei denen die Backend-Anwendung über das Peripheriegerät informiert sein und mit den speziell von diesem Gerät unterstützten Features konfiguriert sein muss.

SDN und OpenFlow bieten ein Hardware- und Software-unabhängiges Abstraktions-Modell für den Zugriff auf Ressourcen und deren Manipulation. Dieses Verfahren umgeht die Produkt-spezifischen Funktionen und verwendet lediglich die Yes/No-Funktionen der Authentifizierung zwischen dem Anwender und der NAC-Anwendung. Sobald der Authentifizierungs-Prozess abgeschlossen ist, wird eine Nachricht an die für die Rollen-basierte Ressourcenzuteilung zuständige SDN-Anwendung gesendet. Diese Nachricht enthält die MAC-Adresse des Anwenders, seinen Zugangs-Port zum Netzwerk und seine Rolle. Die Anwendung vergleicht anschließend diese Rolle mit der zuvor konfigurierten Fähigkeiten-Liste (d. h. mit welchen Anwendern kann dieser Anwender im Netzwerk kommunizieren, welches VLAN sollte diesem Anwender für dieses Netzwerk zugewiesen werden, wie viel Bandbreite kann dem Anwender für seinen Datenverkehr zugewiesen werden, welche IP-Adressen sind für ihn gesperrt, usw.). Diese Fähigkeiten werden in eine Network Resource Message umgewandelt, die an den SDN-Controller gesendet wird. Der SDN-Controller wiederum identifiziert das entsprechende Netzwerk-Gerät, an das die OpenFlow-Tabelle mit den entsprechend zugewiesenen Ressourcen (d. h. Prioritäts-Einstellung für den Datenverkehr, Bandbreite für Datenflüsse) zusammen mit den Limits bezüglich Datenflüssen zu eingeschränkten Adressen gesendet werden soll. Diese Einstellungen werden dann auf dem Port des Brocade ICX 6610 Access Switches gesetzt, sobald der NAC-Server die Authentifizierung des Anwenders auf diesem Port abschließt.

Mit diesem Verfahren können Sie das Peripheriegerät optimieren, ohne die Backend-Systeme anzufassen. Wenn das Peripheriegerät die gleiche OpenFlow-Revision unterstützt wie der SDN-Controller, ist jeder Update für die Rollen-basierte SDN-Anwendung und das Backend völlig transparent. Sobald dem Anwender die Ressourcen zugewiesen wurden, können die standardmäßigen Paketverarbeitungs-Pipelines für das Switching und das Routing der Pakete durch das Netzwerk verwendet werden. Damit kann Brocade eine OpenFlow-Tabelle dazu verwenden, Paketen den Zutritt zum Netzwerk zu erlauben oder zu verweigern und Pakete für spezielle Ressourcen zu markieren (und sie anschließend in die normale Paket-Pipeline zurück zu leiten, wo die Weiterleitungs-Entscheidungen getroffen werden). Für ausgewählte Anwender kann die normale Pipeline auch umgangen und der Datenverkehr über bestimmte Ports geleitet werden.

Ein Beispiel für diesen zweiten Umgebungstyp sind technische Anwender, die an ihrem Arbeitsplatz einen Hochleistungs-Server betreiben. Solche Anwender sind üblicherweise als „vertrauenswürdig“ authentifiziert und können damit den gesamten Datenverkehr von und zu ihrem Server als „sicher“ behandeln lassen. Dieser Datenverkehr darf sich durch das Campus-Netzwerk und über einen leistungsstarken WAN-Link (Wide-Area Network) auf einem Brocade MLXe Router darüber hinaus bewegen, ohne durch eine Firewall passieren zu müssen. Der Datenverkehr aller anderen Anwender, die nicht für diesen „sicheren“ Status authentifiziert sind, wird über die Standard-Pipeline durch eine Firewall abgewickelt, die mit dem MLXe verbunden ist. In diesem Fall sendet der SDN-Controller, sobald er die OpenFlow-Tabelle zu dem Brocade ICX Access Switch sendet, außerdem OpenFlow-Tabellen zu den dazwischenliegenden Brocade ICX und MLX Switches. Dadurch wird eine Pipeline mit garantierter Bandbreite zu dem Brocade MLXe erzeugt, der als der WAN Router agiert, auf dem ein Eintrag so eingestellt ist, dass der gesamte Datenverkehr von diesem Anwender über den Port gesendet wird, der die Firewall umgeht.

Klassische NAC-Systeme kontrollieren nur die Access Layer Switches und lassen den Rest des Netzwerks unberührt. Im Gegensatz dazu verwaltet ein SDN-Controller eine ganzheitliches Mapping des gesamten Netzwerks und der daran angeschlossenen Ressourcen; dadurch können SDN-Anwendungen Zugangs- und Verkehrs-Regeln sehr schnell auf das gesamte Netzwerk anwenden. Durch den Einsatz von Brocade ICX Switches an der Peripherie und im Access Layer und Brocade MLXe Router im Kern ermöglicht Ihnen ein einheitlicher Satz an Funktionalität jenseits von OpenFlow die Trennung des Datenverkehrs priorisierter Anwender vom Datenverkehr „normaler“ Anwender. Damit können Sie entweder die normale Pipeline mit den dazugehörigen Standard-Mechanismen nutzen oder sich für einen vollständigen „OpenFlow-only“ Modus auf Basis eines „Pro-Anwender“-Verkehrsflusses entscheiden. Das bedeutet: NAC bezieht sich nur auf die Ressourcenzuteilung wie VLAN, Access-Control-Lists und eventuell noch QoS-Mechanismen, die aus einem QoS Pool bedient werden. Durch OpenFlow hingegen kann pro Anwender der Datenfluss End-zu-End optimiert werden. Diese Funktionalität bedeutet eine wirklich leistungsstarke Optimierung für die Nutzung der Netzwerk-Ressourcen.

Network Access Control

Der vorherige Use Case „Rollen-basierte Ressourcenzuteilung“ zeigte den Einsatz eines klassischen NAC-Systems für die Anwender-Authentifizierung in Kombination mit SDN, um Anwender-spezifische Zugangs-Regeln zu ermöglichen. Der nächste logische Schritt ist die Implementierung eines vollständigen NAC-Systems mit SDN – damit steht Ihnen die entsprechende Flexibilität zur Verfügung, mehrere Authentifizierungs-Methoden anzubieten und eine Vielzahl von Geräten zu unterstützen.

Der OpenFlow-Standard erlaubt es Ihnen, ein Paket vom SDN-Controller über einen speziellen OpenFlow-fähigen Port auf einem Switch nach außen zu senden. Der Standard ermöglicht es Ihnen außerdem, einen Eintrag in einer OpenFlow-Tabelle zu erzeugen, der dafür sorgt, dass jedes über einen Port empfangene Paket an den SDN-Controller gesendet wird. Diese beiden Features bilden die Bausteine für eine starke NAC-Lösung. Die NAC-Anwendung kann unterschiedliche Authentifizierungs-Verfahren testen, indem sie Pakete versendet, die Protokolle wie z. B. IEEE 802.1X, MAC Authentication oder Web Authentication nachahmen, und kann dann das von dem mit dem Port verbundenen Gerät unterstützte Protokoll verwenden.

Ein Beispiel: Sie haben einige Geräte, die Zugang zu einem gesicherten Netzwerk benötigen; die Geräte verfügen jedoch nicht über die Fähigkeit, auf NAC-Abfragen zu Benutzer/Passwort zu antworten. Dabei kann es sich um Druckserver, Access Points, Lesegeräte für Sicherheitskarten und so weiter handeln. Die MAC-Adresse des jeweiligen Gerät kann

als Authentifizierungs-Verfahren verwendet werden, wobei die Hersteller- und Gerätetyp-Informationen über die MAC-Adresse herausgelesen werden; diese Informationen werden dann mit gültigen Geräten verglichen, die für bestimmte Ports oder einer Reihe von Ports auf bestimmten Switches (die so vorkonfiguriert sind) zugelassen sind. In einem solchen Fall werden vorkonfigurierte Regeln als Einträge in OpenFlow-Tabellen an den betreffenden Switch für den jeweiligen Port gesendet. Dies erlaubt dem Gerät den Zugang zum Netzwerk, beschränkt jedoch die Art von Verkehr, die Zugang zum Netzwerk erhält. So besteht z. B. für ein Kartenlesegerät keine Notwendigkeit, im Internet zu surfen oder Port-Scans auszuführen.

Falls die MAC-Adresse nicht vertrauenswürdig ist, kann versucht werden, das Gerät zu authentifizieren, indem über den Port mit Hilfe der „Packet Insert"-Funktion eine speziell erstellte 802.1X „Session Initiate"-Nachricht an das Gerät gesendet wird. Wenn das Gerät mit dem entsprechenden 802.1X Response Packet antwortet, wird das Paket erfasst, über einen sicheren OpenFlow-Link an den SDN-Controller und von dort an die NAC SDN-Anwendung gesendet. Die NAC-Anwendung simuliert einen RADIUS-Server, vervollständigt den Handshake und authentifiziert den Anwender, indem der SDN-Controller dazu veranlasst wird, die entsprechenden, speziell erstellten Pakete zu senden. An diesem Punkt kommt die Rollen-basierte Ressourcenzuteilung ins Spiel. Anwender mit Geräten, die 802.1X unterstützen, aber derzeit nicht in der Datenbank eingetragen sind, könnten dann abgefragt werden, indem die NAC-Anwendung Standardpakete einspeist, um so eine „Web-Authentifizierung" der Anwender zu simulieren. In anderen Worten: Die NAC-Anwendung simuliert einen DHCP-Server, um eine temporäre IP-Adresse zu vergeben; allerdings fängt sie lediglich den Web-Verkehr vom Anwender ab, simuliert einen Web-Server, und tunnelt die Information über die Webseite, um einen Registrierungsprozess für den Anwender zu starten und ihn zu der 802.1X Datenbank hinzuzufügen. Anschließend wird eine 802.1X Abfrage gestartet; falls diese erfolgreich ist, kann der Anwender dann auf die Ressourcen zugreifen, für die er die Zugriffsrechte hat.

Manchmal gibt es Geräte mit aktiven Anwendern, die jedoch nicht das 802.1X Protokoll verwenden. Bei diesen Geräten funktioniert die Überprüfung der MAC-Adresse der Quelle gegen eine Liste der zugelassenen Geräte nicht. Diese Geräte antworten nicht auf mehrfache 802.1X Abfragen; daher schaltet die NAC-Anwendung auf eine Web-Authentifizierung um. Diese Authentifizierung funktioniert ähnlich der für Geräte, die zwar 802.1X-fähig, aber nicht registriert sind; in diesem Fall jedoch ist jedes Mal, wenn das Gerät Zugang zum Netzwerk braucht, eine Authentifizierung erforderlich. Die NAC-Anwendung ermöglicht dem Anwender zwei Optionen: Login oder Registrierung. Wenn sich der Anwender registriert, folgt er dem gleichen Weg wie die 802.1X-fähigen Anwender. Der Anwender gibt bestimmte Registrierungs-Informationen ein, wählt einen Benutzernamen und ein Passwort und lässt diese an einem Ort speichern, auf den die NAC-Anwendung zugreifen kann. Anschließend wird der Anwender wieder auf die Login- oder Registrierungs-Seite umgeleitet und gibt den Benutzernamen und das Passwort ein. Diese Information wird vollständig durch OpenFlow-Pakete getunnelt, und die OpenFlow-Tabelle wird – nach erfolgreicher Authentifizierung – mit den entsprechenden Tabelleneinträgen konfiguriert, um dem Anwender den Zugang zum Netzwerk mit den entsprechenden Einschränkungen und Ressourcenzuteilungen zu erlauben.

Eine Alternative zum Tunneln der gesamten Webseiten-Funktionalität durch OpenFlow wäre die temporäre Umleitung des gesamten Verkehrs von dem Gerät zu einem Registrierungs-Webserver. Dieser Server könnte alle Web-basierten Registrierungs-Funktionen abwickeln und die Anmeldedaten und Rollen an die NAC-Anwendung senden. Falls es sich um 802.1X Anwender handelt, würde sich der Port-Status ändern, so dass sie sich über die weiter oben beschriebene, simulierte 802.1X-Funktionalität authentifizieren müssten. Falls es sich um Web-basierte Anwender handelt, hätte die NAC-Anwendung die positive Authentifizierung zusammen mit der Rolle des Anwenders empfangen und würde die entsprechenden OpenFlow-Eintrage zum Brocade ICX 6610 senden, um dem Anwender den Zugang zum Netzwerk mit den entsprechenden Einschränkungen und Ressourcenzuteilungen zu erlauben.

Communities of Interest

Communities of Interest (Cols) bestehen aus Gruppen von Individuen, die zusammenarbeiten und sich gemeinsame Ressourcen teilen müssen. Dabei kann es sich um Teams von Wissenschaftlern handeln, die verschiedenen Bereichen des Campus sitzen, funktionsübergreifende Teams, die gemeinsam an einem Projekt arbeiten, externe Dienstleister, Studenten in einem Kurs, oder eine beliebige Anzahl kurzfristiger Gruppierungen, die zusammenarbeiten und sich dedizierte Netzwerk-Ressourcen teilen müssen. Mandantenfähige Anwendungen fallen ebenfalls in diese Kategorie: Dabei handelt es sich um eindeutige Gruppen von Anwendern, die sicher von anderen Gruppen isoliert sind. Solche Gruppen teilen sich eine gemeinsame Architektur; es ist jedoch normalerweise sichergestellt, dass jede Gruppe mit ausreichenden Ressourcen versorgt wird.

Üblicherweise wird dies durch verschiedene Technologien erreicht wie z. B. VLANs (Virtual LANs), die mit VRF-Instanzen (Virtual Routing and Forwarding) mit QoS-Zugriffslisten (Quality of Service) und Rate Limiters verbunden sind. Jedes Mal, wenn dem Netzwerk eine neue Gruppe hinzugefügt wird, braucht es eine gewisse Zeit um festzulegen, wie die Anforderungen dieser Gruppe in das vorhandene Netzwerk eingepasst werden können; außerdem muss jedes betroffene Gerät im Netzwerk kontaktiert werden und die entsprechende Konfiguration angepasst werden. Bei jedem Schritt in diesem Prozess können Fehler auftreten – das Ergebnis sind frustrierte Anwender und stundenlange Fehlersuche; dies beeinträchtigt unnötigerweise die Produktivität der Gruppe und vergeudet Zeit und Geld.

Eine SDN-Lösung reduziert menschliche Fehler und minimiert die Unwägbarkeiten, die durch proprietäre Abhängigkeiten beim Einsatz unterschiedlichster Produkte von unterschiedlichen Herstellern verursacht werden. Unabhängig davon, ob die Gruppe eine statische, langfristige oder eine dynamische, kurzfristige („login, collaborate and logout“) Einrichtung ist: Der SDN-Controller verwaltet den Status der physischen Netzwerk-Topologie, die damit verbundenen Geräte sowie die aktuell zugeteilten Ressourcen. Dadurch ist er in der Lage, die Ressourcen nach Bedarf nahtlos dazu- oder abzuschalten.

Ein Beispiel: Eine Gruppe von Entwicklern beginnt ein auf sechs Monate geplantes Projekt – das neueste Flaggschiff-Produkt für ihr Unternehmen. Die Anwender benötigen von ihren Entwicklungs-Workstations aus eine garantierte Bandbreite. Andere Teams arbeiten in Schichten, verwenden die gleichen Server (aber andere Logins) und gehören zu unterschiedlichen Teams. Das ist ein typisches Szenario für ein kostenbewusstes Unternehmen, das seine Entwicklungs-Workstations maximal auslasten möchte. In einem solchen Szenario könnte jeder Anwender zu einem unterschiedlichen Col-Entwicklungsteam gehören.

Das Verfahren könnte wie folgt funktionieren: Wenn sich ein Anwender an der Workstation anmeldet, werden die gleichen Anmeldedaten für den Login im Netzwerk verwendet, wie in der SDN NAC-Anwendung weiter oben beschrieben. Während der Identifizierung der Anwender werden nicht nur ihre jeweiligen Rollen identifiziert; die CoI-Anwendung stellt außerdem fest, ob ein Anwender zu einer bestimmten, aktiven CoI (Community of Interest) gehört. Die Rollen-basierte Anwendung legt die Sicherheitsauflagen für den Anwenderfest und sendet diese zum SDN-Controller. Die CoI-Anwendung überprüft, welche Anwender aus der CoI (Community of Interest) derzeit angemeldet sind, und fügt die neuen Anwender zu diesem Pool hinzu; diese Information wird anschließend zusammen mit der gewünschten Bandbreite zwischen den Geräten (ebenso wie die Informationen über mögliche aggregierte Bandbreiten, die in Aggregate-/Core-Geräten im Netzwerk reserviert werden sollen) weitergesendet.

Der SDN-Controller nimmt die Anfragen von den Anwendungen entgegen und stellt fest, auf welchen Netzwerk-Geräten die OpenFlow-Tabellen geändert werden müssen, bzw. ob einzelne Einträge am Zugangspunkt oder aggregierte Einträge/Einträge aus Subnetzen in den Aggregation Layers des Netzwerks auf mehrere Anwender in der CoI (Community of Interest) gemappt sind. Anschließend „pusht“ der Controller all diese Tabelleneinträge zu den jeweiligen Geräten. Das alles passiert, während sich der Anwender an der Workstation anmeldet und die erste Datei öffnet – und der Prozess ist für den Anwender völlig unsichtbar.

Wenn sich der Anwender vom Gerät abmeldet, wird der Prozess rückwärts durchlaufen. Die CoI (Community of Interest) und die Rollen-basierten Anwendungen teilen dem SDN-Controller mit, dass er die Ressourcen für den Anwender herunterfahren kann, und der SDN-Controller stellt fest, welche Geräte geändert werden müssen. Der Controller „pusht“ anschließend die entsprechenden Tabelleneinträge auf den Aggregation Layer und gibt die Ressourcen auf dem Access Switch wieder frei. Niemand muss sich Gedanken über ACL-Einträge, CLI-Einschränkungen (Command-Line Interface) oder darüber machen, wie vielen Anwendern bereits Bandbreite auf diesem Link zugeteilt wurde. Der SDN-Controller erledigt das alles für Sie – mit einem physischen und logischen Mapping der Ressourcen und der OpenFlow API.

DIE LÖSUNG VON BROCADE

Brocade ist der Vorreiter bei der Weiterentwicklung von SDN – von einfachen Testumgebungen bis hin zur Bereitstellung in „Real Life“-Netzwerken. Die ersten Brocade-Produkte waren die Brocade NetIron® CES, CER und MLX Plattformen für den Einsatz im Core bzw. an der WAN-Peripherie. Diese umfassten auch den Hybrid Per-Flow-Modus, der die Elastizität, die Brocade in zwanzig Jahren der Hardware- und Software-Entwicklung im Bereich Verkehrsfluss-Management gewonnen hatte, mit der Agilität von OpenFlow kombiniert; damit können bestimmte Datenflüsse von Anwendungen und Anwendern dynamisch und sehr exakt abgestimmt werden. Die erste Release war eine erweiterte Version von OpenFlow Version 1.0. Die aktuellen und künftigen Produkte implementieren OpenFlow Version 1.3 inklusive den verbesserten Möglichkeiten in den Bereichen Funktionalität, Hochverfügbarkeit und Sicherheit.

Dank der NetIron-Produkte konnte Brocade die Geräte optimal auf die Performance der SDN-Controller einstellen und den Betrieb im Hybrid Per-Flow-Modus zu einer stabilen, einsatzfähigen Lösung der Enterprise-Kasse weiterentwickeln. Diese Fähigkeiten stehen inzwischen auch in den Brocade ICX Campus-Produkten und den Brocade Data Center Ethernet Fabric VDX Produkten zur Verfügung. Außer den Routern der Brocade MLX-Serie

für den Core und die WAN-Plattform wird der Brocade ICX 6610 die SDN-Produktpalette von Brocade erweitern. Damit steht nicht nur ein robuster, OpenFlow-fähiger Access Switch mit PoE (Power over Ethernet), sondern auch ein leistungsstarker Switch für den Aggregation Layer oder in kleinen Cores, und ein stabiler ToR-Switch (Top of Rack) für Front-End-Server im Rechenzentrum zur Verfügung. Brocade engagiert sich sehr stark in den Bereichen SDN und OpenFlow und wird daher die OpenFlow-Funktionalitäten in der Brocade ICX-Familie weiter ausbauen, um in unternehmensweiten Campus-Netzwerken eine wirklich skalierbare Topologie zu ermöglichen. Die Brocade VDX-Serie bietet außerdem „Flow to Optimal Fabric Path Mapping“. Das Ergebnis ist eine umfassende, dynamische Netzwerk-Topologie für SDN-Anwendungen, die bis dato nicht orchestriert werden konnten.

ZUSAMMENFASSUNG

Brocade erkannte sehr früh die Möglichkeiten, die SDN für die Anpassung des Netzwerks an das 21ste Jahrhundert für Anwendungen des 21sten Jahrhunderts bietet. Diese Änderung ist vergleichbar mit dem Übergang von DOS zu Windows; d. h. der Übergang von einem „wir wissen viel zu viel darüber, wie die Hardware funktioniert“ hin zum Einsatz von Software, ohne sich der darunterliegenden Hardware bewusst zu sein – bzw. ohne darüber Bescheid wissen zu müssen. Brocade ist sich durchaus bewusst, dass in dieser Übergangsphase „Alt“ und „Neu“ nebeneinander existieren und eine Migration von „Alt“ nach „Neu“ ermöglicht werden muss. Der Hybrid Per-Flow-Modus ist nur eine der vielen Innovationen von Brocade. Er ermöglicht einen kontrollierten, gleitenden Übergang zu einem SDN-Ökosystem mit Produkten, die nahtlos mit der vorhandenen Netzwerk-Topologie zusammenarbeiten; gleichzeitig stehen Ihnen alle Möglichkeiten offen, SDN in Ihrem Netzwerk zu implementieren – zu Ihren eigenen Bedingungen, in einer Geschwindigkeit Ihrer Wahl. Brocade bietet eine breite Palette OpenFlow-fähiger Netzwerk-Komponenten – vom On-ramp Access Layer des Campus-Netzwerks bis hin zum Server im Rechenzentrum. Des weiteren engagiert sich Brocade aktiv in den Normengremien. Brocade ist über das Open-Source SDN Controller Consortium einer der Champions der Enterprise User Viewpoint, um eine stabile, kostengünstige Lösung der Enterprise-Klasse zu gewährleisten. Brocade unterstützt außerdem Anwendungs-Entwickler im Bereich SDN mit dem Ziel, eine vollständige Suite von Enterprise-Lösungen sicherzustellen. Brocade bekennt sich auf allen Ebenen zu SDN: Netzwerk-Komponenten, stabile SDN-Controller und SDN-Anwendungen der Enterprise-Klasse – für eine umfassende Lösung, die die hohen unternehmerischen Anforderungen von heute und morgen erfüllt.

ÜBER BROCADE

Brocade Netzwerklösungen helfen Unternehmen dabei, beim reibungslosen Übergang in eine Welt, in der sich Anwendungen und Informationen überall befinden können, auch ihre wirtschaftlichen Ziele zu erreichen. Brocade dehnt seine bewährte Kompetenz im Rechenzentrum auf das gesamte Netzwerk aus – mit offenen, virtuellen und effizienten Lösungen, ausgelegt auf Konsolidierung, Virtualisierung und Cloud Computing.
Weitere Informationen finden Sie auf www.brocade.com.

Corporate Headquarters
San Jose, CA USA
T: +1-408-333-8000
info@brocade.com

European Headquarters
Genf, Schweiz
T: +41-22-799-56-40
emea-info@brocade.com

Deutschland
Garching bei München
T: +49-89-20000-9100
infode@brocade.com

BROCADE