Informationen auf einen Blick

Vorteile

Für Endbenutzer

- Hochgradig sicherer Zugriff für alle gängigen Mobilgeräte
- Konsistentes Benutzererlebnis
- Intelligente, zuverlässige und stets verfügbare Verbindungen

Für Sicherheitsadministratoren

- Höhere Produktivität und niedrigere Gesamtbetriebskosten durch einen Client, der alles vereint
- Kontextbezogene, umfassende und einfache Durchsetzung von Sicherheitsrichtlinien
- Flexibler, richtliniengesteuerter Zugriff auf Unternehmensressourcen und -anwendungen für jede Benutzergruppe und jedes Gerät über Kabel-, Wireless- und VPN-Netzwerke

Cisco AnyConnect Secure Mobility Client

Ganz gleich, ob Ihre Mitarbeiter unternehmenseigene Laptops oder private Mobilgeräte verwenden – wenn Sie standortunabhängiges Arbeiten ermöglichen möchten, muss dabei stets die Sicherheit der Daten Ihres Unternehmens gewährleistet sein. Möglich wird dies mit dem Cisco AnyConnect® Secure Mobility Client (Abbildung 1), einem umfassenden Agent, der verschiedenste Security-Services bereitstellt und Ihnen die erforderliche Transparenz und Kontrolle liefert, um festzustellen, wer und was auf Ihr erweitertes Unternehmensnetzwerk zugreift – vor, während und nach einem Angriff. Der AnyConnect® Secure Mobility Client vereint Remote-Zugriff, Statusdurchsetzung und Web-Sicherheit in einer umfassenden Plattform für die Endpunkt-Sicherheit, die alle Funktionen bietet, die Ihre IT-Abteilung für die Bereitstellung einer stabilen, benutzerfreundlichen und hochgradig sicheren Umgebung für mobile Benutzer benötigt.

Abbildung 1: AnyConnect Secure Mobility Client

Funktionen und Vorteile

Der branchenführende AnyConnect Secure Mobility Client ist äußerst vielseitig. Denn diese Endpunkt-Software ermöglicht nicht nur VPN-Zugriff über Secure Sockets Layer (SSL) und IPsec IKEv2, sondern erhöht die Sicherheit zusätzlich durch zahlreiche integrierte Module. Diese bieten Services wie Compliance durch die VPN- und Cisco ISE-Statusprüfung (Identity Services Engine), Web-Sicherheit, Netzwerktransparenz und den Network Access Manager. AnyConnect ist für eine breite Palette an Plattformen verfügbar, darunter Windows, Mac OS X, Linux, iOS, Android, Windows Phone, BlackBerry und Google Chrome (Preview).

Nächste Schritte

Weitere Informationen finden Sie auf den folgenden Websites:

- Lizenzierung und Bestellung: Die Lizenzierung für AnyConnect, Clientless-SSL-VPN und Internet Key Exchange Version 2 (IKEv2) Remote-Access-VPNs von Drittanbietern wird in der Bestellanleitung zu Cisco AnyConnect erläutert.
- Cisco AnyConnect Secure Mobility Client: http://www.cisco.com/go/anyconnect
- Cisco Serie ASA 5500-X: http://www.cisco.com/go/asa

Tabelle 1 zeigt die wichtigsten Funktionen.

Tabelle 1: Funktionen des AnyConnect Secure Mobility Client

Funktion	Beschreibung
Einheitliche Endpunkt-Compliance	Der AnyConnect ISE Agent stellt in Verbindung mit der Cisco ISE eine einheitliche Endpunkt-Statusprüfung und -Problembehebung in allen kabelgebundenen, Wireless- und VPN-Umgebungen sicher. Als zentrale Quelle für die Prüfung auf Betriebssystemversionen, die neuesten Antivirus-Updates und andere Ressourcen stärkt er die Endpunkt-Sicherheit und -Compliance. Die Endpunkt-Statusprüfung ist darüber hinaus mit Cisco Hostscan auch über die Adaptive Security Appliance verfügbar.
Hochgradig sicherer Netzwerkzugriff	Mit den herausragenden Funktionen des AnyConnect Network Access Manager können Administratoren kontrollieren, mit welchen Netzwerken oder Ressourcen Endpunkte eine Verbindung herstellen dürfen. Er bietet einen IEEE 802.1X-Supplicant, der in Verbindung mit AAA-Funktionen (Authentication, Authorization, Accounting) und leistungsstarken Verschlüsselungstechnologien wie MACsec IEEE 802.1AE bereitgestellt werden kann.
Web-Sicherheit	AnyConnect beinhaltet ein integriertes Modul, das Web-Sicherheitsfunktionen entweder über die standortbasierte Cisco Web Security Appliance (WSA) oder Cloud-basiert über Cisco Cloud Web Security implementiert. Durch die Kombination von Web-Sicherheit und VPN-Zugriff können Administratoren eine umfassende, hochgradig sichere Mobility-Umgebung für alle Endbenutzer gewährleisten – eine entscheidende Voraussetzung für BYOD (Bring-Your-Own-Device). Zum Schutz vor Web-Malware und zur Kontrolle und Absicherung der Web-Nutzung stehen zahlreiche Bereitstellungsoptionen zur Verfügung.
Netzwerk-transparenz	Das AnyConnect Network Visibility-Modul auf Windows- und Mac OS X-Plattformen ermöglicht Administratoren die Überwachung der Anwendungsnutzung von Endpunkten. Anhand dieser Informationen können sie potenziell ungewöhnliches Verhalten ermitteln und das Netzwerkdesign optimal anpassen. Zudem stehen immer mehr IPFIX-fähige (Internet Protocol Flow Information Export) Netzwerkanalysetools zur Verfügung, die diese Nutzungsdaten ebenfalls nutzen können.
Clientless-Zugriff	Mit Cisco Adaptive Security Appliances können zahlreiche unterschiedliche Browser und Plattformen für die Verbindung via SSL verwendet werden. Hierzu können Administratoren den Clientless-VPN-Zugriff für nicht verwaltete Endpunkte einrichten und Zugriff auf eine Vielzahl von Web- und TCP/IP-basierten Anwendungen ermöglichen. Der Zugriff erfolgt unter Nutzung der in den Browser integrierten SSL-Technologie mittels Rewriter, Plug-ins oder Smart Tunnels, wobei eine präzise Zugriffskontrolle und End-to-End-Sicherheit jederzeit gewährleistet sind.
VDI-Zugriff (Virtual Desktop Infrastructure)	Cisco ASAs bieten ein hohes Maß an Sicherheit bei der Terminierung von VDI-Sitzungen und ermöglichen einen transparenten Zugriff auf virtualisierte Anwendungen und Desktops, der über Mobilgeräte, Laptops und Desktop-PCs sowohl clientbasiert als auch clientless erfolgen kann. Der hochgradig sichere Remote-Zugriff ist dabei anbieterunabhängig und wird von einer einheitlichen Richtlinie gesteuert, die für virtuelle und physische Ressourcen gleichermaßen gilt.
Mobilgeräte-Unterstützung	Im Zuge des BYOD-Trends müssen Administratoren den Zugriff auf das Unternehmensnetzwerk auch über private Mobilgeräte ermöglichen, damit die Mitarbeiter produktiv bleiben können. AnyConnect unterstützt alle gängigen Mobilgeräte und ermöglicht einen hochgradig sicheren Remote-Zugriff entweder auf Gerätebasis oder transparent nur für ausgewählte Anwendungen via Per-Application-VPN. Das neue Per-Application-VPN verhindert, dass nicht genehmigte Anwendungen auf vertrauliche geschäftliche Ressourcen zugreifen können. Das reduziert das Risiko von Malware-Infektionen sowie die Bandbreitenkosten für den Remote-Zugriff.

C45-578609-06 10/15