Ihre besten 6 Wochen
Vom Produkt zur Lösung

Top Konditionen für Cisco Security-Lösungen

6 geschäftliche Gründe dafür, sichere Netzwerke zu verkaufen

1. **Sie sollten wissen, wer Verbindung zu Ihrem Netzwerk aufnimmt**
   Wissen Sie, wer sich in Ihr Netzwerk einwählt, und ob Ihr Unternehmen so der Gefahr durch sog. „Malware" auf dem Internet ausgesetzt wird?
   Mit dem NAC (Network Admission Control) Modul für den 2811 „Internet facing" Router können Sie überprüfen, wer aus Ihrer Organisation heraus das Internet aufruft und ob hierfür die richtige Software verwendet wird. So lässt sich die bösartige „Malware" vermeiden, die von manchen Websites ausgeht.
2. **Sicherer Zugriff, auch unterwegs**
   Ihre mobilen Mitarbeiter wollen auch dann schnell und sicher Verbindung zu Ihrem Unternehmen aufnehmen können, wenn sie unterwegs sind. Gleichzeitig benötigt Ihr Security-Team leistungsstarke Tools für Authentifizierung und die Kontrolle der Einhaltung von Richtlinien.
   Der ASA 5505, zertifiziert nach Common Criteria EAL4, bietet einen VPN Terminierungspunkt für SSL VPNs und IPSec VPNs, sodass mobile Anwender eine sichere Verbindung zum Unternehmen herstellen können.
3. **Schutz von geschäftskritischen Daten**
   Zahlreiche Richtlinien geben den nachweisbaren Schutz von geschäftskritischen Daten vor. Unternehmen müssen somit Sicherheitsmechanismen implementieren, mit denen die Einhaltung dieser Richtlinien belegt werden kann.
   Die Cisco® ASA 5500 Series Intrusion Prevention System (IPS) Lösung schützt die entscheidenden Informationen Ihres Unternehmens.
4. **Konstruktive Internetnutzung durch Ihre Mitarbeiter**
   Die unangemessene Nutzung des Internets kann zu Produktivitätsverlusten für Unternehmen führen. Bösartige Malware auf Websites und eventuelle rechtliche Schritte, falls unangemessene Materialien aufgerufen wurden, können Ausfallzeiten und Umsatzverluste verursachen.
   Der ISR 1841 soll eine Plattform bieten, die integrierte IPS Modul-Funktionalität enthält und nicht nur vor Malware schützt, sondern auch IOS Content Filtering nutzt, um den Zugriff auf ungeeignete URLs zu vermeiden.
5. **E-Mail schützen**
   Diese Cisco Business Security Lösung schützt vor Bedrohungen, die per Email und über das Web kommen, und zwar mit Hilfe der ASA 5500 Series Content Security Edition. Dies baut auf einer Partnerschaft mit Trend Micro auf, um Antivirus- und Anti-Spyware-Funktionalität zu bieten. Dabei besteht die Möglichkeit eines Upgrades auf Anti-Spam-, Anti-Phishing-, URL Blocking-, Content Filtering- und E-Mail Content Filtering-Funktionalität innerhalb einer Unified Threat Management Plattform. Hierfür wird das leistungsstarke ASA Device Manager Tool verwendet.
6. **Hohe Netzwerkverfügbarkeit während der Geschäftszeiten**
   Unternehmen verlassen sich darauf, dass ihr Netzwerk eine Reihe von Hochverfügbarkeitsfunktionen bietet und so rund um die Uhr für hohe betriebliche Produktivität sorgt.
   Der 1841 ISR mit seinen modularen Steckplätzen ermöglicht die Installation von primären und Backup-WAN/Redundant Interface-Optionen, um – je nach Anforderungen der Kunden - E1-, ADSL-, V.92- oder ISDN-Technologien einsetzen zu können.

1. Sie sollten wissen, wer Verbindung zu Ihrem Netzwerk aufnimmt

Wissen Sie, wer sich in Ihr Netzwerk einwählt, und ob Ihr Unternehmen so der Gefahr durch sog. „Malware“ auf dem Internet ausgesetzt wird?
Diese Cisco Business Security-Lösung enthält das NAC (Network Admission Control) Modul für den 2811 „Internet facing“ Router. Hiermit können Sie überprüfen, wer aus Ihrer Organisation heraus das Internet aufruft und ob hierfür die richtige Software verwendet wird. So lässt sich die bösartige „Malware“ vermeiden, die von bestimmten Websites ausgeht.

Mit NAC können Kunden den Netzwerkzugriff auf bekannte Endpunkte beschränken, die den relevanten Richtlinien entsprechen (z.B. PCs, Server und PDAs) und die Zugriffsmöglichkeiten für andere Geräte einschränken. Netzwerkadministratoren können über Kabel, drahtlos oder „remote“ angeschlossene Benutzer und ihre Maschinen authentifizieren, autorisieren, überprüfen und eventuelle Probleme beheben, bevor ihnen der Zugang zum Netzwerk ermöglicht wird. Dieses weit verbreitete Sicherheitstool integriert Zugang auf Basis der Identität, Einschätzung von Schwachstellen, Policy Management und Patch Management in einem Modul und senkt so die Betriebskosten, die mit der Implementierung von separaten Geräten verbunden wären.

Technologie	Produkt	Beschreibung
Switching	WS-C2960G-48TC-L	Cisco Catalyst 2960G-48TC-L mit LAN Base SW: Festkonf. StandaloneSwitch: 44 10/100/1000 Ports und 4 Dual-Purpose 10/100/1000 Uplink Ports (BASE-T/SFP)
Sicherheit	ASA5505-50BUN-K9	Cisco ASA 5505 Firewall Edition - 50 User Bundle: 50 User Firewall, 10 IPSec VPN- und 2 SSL-VPN-Anwendersitzungen, 3DES/AES Lizenz, 8-Port 10/100 Fast Ethernet Switch (davon 2 mit PoE), 3 VLANs, SSC-Erweiterungsslot
Routing	CISCO2811SEC/K9	Integrated Services Router 2811 Security Bundle, Advanced Security, 64F/256D
	S28NUASK9A-12415T	Cisco 2800 ASK9-AESK9 FEAT SET FACTORY UPG FOR BUNDLES
	NME-NAC-K9	Cisco NAC Netzwerkmodul für 2800, 3800 ISR
	NACNM-SW41-K9	AC Netzwerkmodul Version 4.1t
	NACNM-50-K9	NAC Netzwerkmodul Serverlizenz – max. 50 User

Die Cisco ASA 5500 Series Firewall Edition bietet:

- Eine breite Palette von Services für die Sicherung von modernen Netzwerkumgebungen
- Sicheren „Site-to-Site“ und „Remote User“-Zugriff auf Unternehmensnetzwerke und Services
- Ein modulares Design, das an die Entwicklung eine Unternehmens angepasst werden kann
- Eine große Auswahl von intelligenten Networking-Services, um eine nahtlose Integration in die unterschiedlichsten Netzwerkumgebungen zu ermöglichen

2. Damit Ihre Mitarbeiter auch unterwegs sicher auf Ihr Netzwerk zugreifen können

Ihre mobilen Mitarbeiter wollen auch dann schnell und sicher Verbindung zu Ihrem Unternehmen aufnehmen können, wenn sie unterwegs sind. Gleichzeitig benötigt Ihr Security-Team leistungsstarke Tools für die Authentifizierung und die Kontrolle der Einhaltung von Richtlinien.

Diese Cisco Business Security-Lösung verwendet den ASA 5505, zertifiziert nach Common Criteria EAL4, um einen VPN Terminierungspunkt für SSL VPNs und IPSec VPNs zu bieten. So können mobile Anwender eine sichere Verbindung zum Unternehmen herstellen.

Konnektivität ist über den automatisch heruntergeladenen Cisco AnyConnect VPN Client, den Cisco IPsec VPN Client und die Microsoft und Mac OS X Layer 2 Tunneling Protocol (L2TP)/IPsec VPN Clients möglich.
Der Cisco AnyConnect VPN Client passt sein Tunneling-Protokoll automatisch an die effizienteste Methode an und berücksichtigt dabei die Einschränkungen des Netzwerks. Es handelt sich hierbei um das erste VPN-Produkt, welches das DTLS-Protokoll einsetzt, um eine optimierte Verbindung für latenzempfindlichen Verkehr bereit zu stellen. Hierbei könnte es sich z.B. um VoIP (Voice over IP) Verkehr oder Anwendungszugriff auf TCP-Basis handeln. Indem sie SSL, DTLS und IPsec-basierte Remote-Access VPN Technologien unterstützt, bietet die Cisco ASA 5500 Serie bisher unerreicht Flexibilität und kann so in den unterschiedlichsten Implementierungsszenarien eingesetzt werden.

Mit dem 1801 ADSL Router können Unternehmen von den schnellen ADSL-Leitungen in ihren Büros profitieren. Gleichzeitig sorgt die integrierte Intrusion Prevention System-Funktionalität dafür, dass die Organisation vor externen, bösartigen Bedrohungen geschützt wird. Die Software-Firewall bietet zusätzliche Sicherheit.

Technologie	Produkt	Beschreibung
Switching	WS-C2960G-48TC-L	Cisco Catalyst 2960G-48TC-L mit LAN Base Software: Festkonf. Standalone Switch: 44 10/100/1000 Ports und 4 Dual-Purpose 10/ 100/ 1000 Uplink Ports (BASE-T/SFP)
Sicherheit	ASA5505-50-BUN-K9	Cisco ASA 5505 Firewall Edition - 50 User Bundle: 50 User Firewall, 10 IPSec VPN- und 2 SSL-VPN-Anwendersitzungen, 3DES/AES Lizenz, 8-Port 10/100 Fast Ethernet Switch (davon 2 mit PoE), 3 VLANs
Routing	CISCO1801/K9	Cisco Integrated Services Router 1801 Adv. IP Services: Empfohlen bis 50 User; WAN Ports ADS-LoPOTS + Fast Ethernet,Fire-wall, Switch, IPS,NAC, VPN,QoS

3. Schutz von geschäftskritischen Daten

Zahlreiche Richtlinien geben den nachweisbaren Schutz von geschäftskritischen Daten vor. Unternehmen müssen somit Sicherheitsmechanismen implementieren, mit denen die Einhaltung dieser Richtlinien belegt werden kann.

Diese Cisco Business Security-Lösung verwendet die Cisco® ASA 5500 Series Intrusion Prevention System (IPS) Solution, um Ihre geschäftskritischen Informationen optimal zu schützen. Hierzu werden branchenführende IPS- und Firewall-Technologie sowie Cisco® IPS Manager Express (IME) eingesetzt. Hierbei handelt es sich um einen komplette IPS Management-Anwendung, die Policy- und Event-Management speziell für die Anforderungen von kleinen und mittleren Unternehmen bietet.

Die Cisco ASA IPS-Lösung erweitert den Firewall-Schutz, indem sie Bedrohungen wie Würmer, trojanische Pferde, Viren, Distributed Denial of Service, Erkundungsversuche und Angriffe auf Schwachstellen des Betriebssystems und der Anwendungen abwendet. Mit Hilfe von Cisco Anomaly Detection und Cisco Services for IPS Signatur-Updates, die von einem weltweiten Team rund um die Uhr zur Verfügung gestellt werden, kann die Cisco ASA 5500 Series IPS-Lösung schnell angepasst werden, um neue Bedrohungen zu identifizieren und zu stoppen. Dies trägt zum Schutz Ihrer Ressourcen und Ihres Netzwerks bei.

Technologie	Produkt	Beschreibung
Switching	WS-C2960-24TC-S	Cisco Catalyst 2960-24TC-S mit LAN Lite Software: Festkonf. Standalone-Switch: 24 10/100 Ports und 2 Dual-Purpose 10/100/1000 Uplink Ports (BASE-T oder SFP)
Sicherheit	ASA5510-AIP10-K9	Cisco ASA 5510 IPS Edition inkl. AIP-SSM-10 Modul für Intrusion Prevention Services, Firewall, 250 IPSec VPN-Peers, 2 SSL-VPN Peers, 3DES/AES, 50 VLANs
Routing	CISCO 1811/K9	Services Router 1811 Adv. IP Services: Empfohlen bis 50 User; 2 Fast Ethernet WAN Ports; Firewall, IPS, NAC, IPSec VPN 50 Tunnel, QoS

Der Cisco 1811 hat ein integriertes v.92 Modem für analoges Backup auf das Dual Ethernet WAN, während der integrierte Switch 8 Ports mit 10/100Base-T unterstützt. Der Cisco 1811 macht die Netzwerkinfrastruktur von mittelständische Unternehmen und Filialen von Großunternehmen möglich und bietet Zugang zum Internet, der Unternehmenszentrale und anderen Filialen. Gleichzeitig sichert und schützt er geschäftskritische Daten mit integrierten Cisco IOS Software-Sicherheitsfunktionen.

4. Konstruktive Internetnutzung durch Ihre Mitarbeiter

Die unangemessene Nutzung des Internets kann zu Produktivitätsverlusten für Unternehmen führen. Bösartige Malware auf Websites und eventuelle rechtliche Schritte, falls unangemessene Materialien aufgerufen wurden, können Ausfallzeiten und Umsatzverluste verursachen.

Diese Cisco Business Security-Lösung verwendet den ISR 1841, um eine Plattform zu bieten, die integrierte IPS Modul-Funktionalität enthält und nicht nur vor Malware schützt, sondern auch IOS Content Filtering nutzt, um den Zugriff auf ungeeignete URLs zu vermeiden. Cisco IOS Content Filtering ist ideal für mittelständische Unternehmen und Filialen von Großunternehmen geeignet, die eine skalierbare Lösung mit niedrigem Wartungsaufwand benötigen. Cisco IOS Content Filtering bietet Bewertungen oder „Ratings" von Produktivität und Sicherheit auf der Basis von bestimmten Kategorien. „Content-aware" Sicherheitsbewertungen schützen vor Malware, bösartigem Code, Phishing-Angriffen und Spyware. Die Blockierung von bestimmten URLs und Keywords trägt dazu bei, dass Ihre Mitarbeiter produktiv mit dem Internet arbeiten. Dies ist eine gehostete Lösung, deren Nutzung regelmäßig verlängert wird. Sie nutzt die globale TrendLabs™ Bedrohungsdatenbank von Trend Micro und ist eng mit Cisco IOS integriert.

Technologie	Produkt	Beschreibung
Switching	WS-C2960-48TT-L	Cisco Catalyst 2960-48TT-L mit LAN Base Software: Festkonfigurierter Standalone-Switch: 48 10/100 Ports und 2 10/100/1000 Uplink Ports
Sicherheit	ASA5505-SEC-BUN-K9	Cisco ASA 5505 Firewall Edition-Security Plus- Unlimitierte User: Unlimitierte User Firewall, 25 IPSec VPN- und 2 SSL-VPN Anwendersitzungen, 3DES/AES, DMZ, Stateless Active/Standby high availability, 8-Port 10/100 Fast Ethernet Switch (davon 2 mit PoE), 20 VLANs
Routing	CISCO1841-HSEC/K9	Cisco Integrated Services Router 1841 Adv.IP Services mit AIM-VPN/SSL-1 (IPSec VPN+SSL), 10 User Lizenz SSL, Modularer Router, QoS, Firewall, IPS, NAC, Erfordert Content Filter Lizenz und 12.4(20)T

Die Cisco ASA 5500 Series Firewall Edition bietet:

- Eine breite Palette von Services für die Sicherung von modernen Netzwerkumgebungen
- Sicheren „Site-to-Site" und „Remote User"-Zugriff auf Unternehmensnetzwerke und Services
- Ein modulares Design, das an die Entwicklung eine Unternehmens angepasst werden kann
- Eine große Auswahl von intelligenten Networking-Services, um eine nahtlose Integration in die unterschiedlichsten Netzwerkumgebungen zu ermöglichen

5. Email schützen

Unternehmen und Mitarbeiter sind kontinuierlich Bedrohungen ausgesetzt, die entweder in ihren E-Mails enthalten sind oder in Form von Malware auf bestimmten Websites auf sie warten.

Diese Cisco Business Security Lösung schützt vor Bedrohungen, die per Email und über das Web kommen, und zwar mit Hilfe der ASA 5500 Series Content Security Edition. Dies baut auf einer Partnerschaft mit Trend Micro auf, um so Antivirus- und Anti-Spyware-Funktionalität zu bieten. Dabei besteht die Möglichkeit eines Upgrades auf Anti-Spam-, Anti-Phishing-, URL Blocking-, Content Filtering- und E-Mail Content Filtering-Funktionalität innerhalb einer Unified Threat Management Plattform. Hierfür wird das leistungsstarke ASA Device Manager Tool verwendet.

Technologie	Produkt	Beschreibung
Switching	WS-C2960-24TC-L	Cisco Catalyst 2960-24TC-L mit LAN Base Software: Festkonf. Standalone-Switch: 24 10/100 Ports und 2 Dual-Purpose 10/100/1000 Uplink Ports (BASE-T/ SFP)
Sicherheit	ASA5510CSC10-K9	Cisco ASA 5510 Anti-X Edition inkl. CSC-SSM-10 Modul mit 50 User Antivirus + Anti-Spyware Lizenz für 1 Jahr, Firewall, 250 IPSec VPN-Peers, 2 SSL-VPN Peers, 3DES/AES, 50 VLANs
Routing	CISCO1841-SEC/K9	Cisco Integrated Services Router 1841 Advanced Security Bundle: Empfohlen bis 50 User, Modularer Router, QoS, Firewall, IPSec VPN 100 Tunnel, IPS, NAC)

Der Cisco 1841 Integrated Services Router, Teil der preisgekrönten Cisco 1800-Serie, eignet sich ideal für mittelständische Unternehmen. Er ermöglicht es ihnen,

Kosten zu reduzieren, indem sie ein einzelnes, belastbares System implementieren, das schnell und sicher mehrere geschäftskritische Business Services bereitstellt. Integrierte Sicherheit ist dabei natürlich Teil dieser Dienste.

6. Hohe Netzwerkverfügbarkeit während der Geschäftszeiten

Unternehmen verlassen sich darauf, dass ihr Netzwerk eine Reihe von Hochverfügbarkeitsfunktionen bietet und so rund um die Uhr für hohe betriebliche Produktivität sorgt.

Diese Cisco Business Security-Lösung verwendet den 1841 ISR mit seinen modularen Steckplätzen, um so die Installation von primären und Backup- WAN/Redundant Interface-Optionen zu ermöglichen. So können, je nach Anforderungen der Kunden, E1-, ADSL-, V.92- oder ISDN-Technologien eingesetzt werden. Cisco IOS enthält zahlreiche IOS Sicherheitsfunktionen, um die Verfügbarkeit des Routers auch dann zu gewährleisten, wenn er angegriffen wird. Control Plane Policing reduziert die Auswirkungen von DDOS-Angriffen auf den Router, während andere Sicherheitsfunktionen wie Authentifizierung, rollen-basierte CLI, RFC2927 Filtering und ACLs dafür sorgen, dass sich die Auswirkungen von unautorisiertem Zugriff und Hacking-Versuchen in Grenzen halten.

Technologie	Produkt	Beschreibung
Switching	WS-C2960-24PC-L	Cisco Catalyst 2960-24PC-L PoE LAN Base Software: Festkonf. Standalone-Switch, 24 10/100 Ports PoE und 2 Dual-Purpose 10/100/1000 Uplinks (BASE-T/ SFP)
Sicherheit	ASA5510-SEC-BUN-K9	Cisco ASA 5510 Firewall Edition Security Plus: Firewall, 250 IPSec VPN-Peers, 2 SSL-VPN Peers, Security Plus
Routing	CISCO1841-T1	Cisco Integrated Services Router 1841 T1 Bundle (inkl. WAN Interface Card WIC-1DSU-T1-V2): Empfohlen bis 50 User, IP Base, Modularer Router, QoS

Die ASA 5510 Firewall ist mit einer „High Availability" Lizenz konfiguriert. Dies ermöglicht den Kauf einer identischen Einheit, sodass eine hoch verfügbare Firewall-Lösung bereitgestellt werden kann. Die Lizenz erlaubt Active/Active* oder Active/ Standby-Funktionen bei virtuellen Firewalls. *Active/ Active bedeutet, dass sich eine virtuelle Firewall im Active-Modus und die dazugehörige virtuelle Firewall im Standby-Modus befindet.

Auf dem Catalyst 2960 Switch sind 24 Power over Ethernet Ports installiert, sodass er Wirless Access Points oder IP-Telefone mit Strom versorgen kann. So lassen sich unnötige Stromkabel oder Steckdosen in der Nähe der Endgeräte vermeiden.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**