

Cisco IOS-Software: Firewall-Funktionsgruppe

DA DIE NETZWERKSICHERHEIT EINE IMMER GRÖßERE BEDEUTUNG BEI DER SICHERUNG VON GESCHÄFTSTRANSAKTIONEN GEWINNT, MÜSSEN UNTERNEHMEN DIE SICHERHEIT DIREKT IN DAS NETZWERKDESIGN UND DIE INFRASTRUKTUR INTEGRIEREN. DIE EINHALTUNG VON SICHERHEITSREGELN IST AM EFFEKTIVSTEN, WENN SIE EIN EIGENER BESTANDTEIL DES NETZWERKS IST.

Cisco IOS®-Software ist auf mehr als 80 Prozent aller Internet-Backbone-Router installiert und wird dadurch zur wichtigsten Komponente der heutigen Netzwerkinfrastruktur. Die auf Cisco IOS-Software basierende Sicherheit bietet die beste Lösung für Ende-zu-Ende-Netzwerksicherheit für Internet, Intranet und Fernzugriff.

Die Cisco IOS Firewall ist Teil der Cisco Secure-Produktfamilie und eine spezifisch auf Sicherheit ausgerichtete Option für die Cisco IOS-Software. Sie integriert robuste Firewall-Funktionen und Angriffserkennung für die gesamte Netzwerkperipherie und verbessert die vorhandenen Cisco IOS-Sicherheitsfähigkeiten. Sie erweitert vorhandene Cisco IOS-Sicherheitslösungen wie Authentisierung, Verschlüsselung und Failover um größere Tiefe und Flexibilität durch modernste Sicherheitsmechanismen wie verbindungsorientiertes, anwendungsbasiertes Filtern, dynamische benutzerspezifische Authentisierung und Autorisierung, Verteidigung gegen Netzwerkangriffe, Java-Blockierung und Echtzeitalarm. In Kombination mit der Cisco IOS IP Security- (IPSec)-Software und anderen auf Cisco IOS-Software basierenden Techniken wie dem Layer 2 Tunneling Protocol (L2TP) und der Dienstgüte (Quality of Service, QoS) stellt die Cisco IOS Firewall eine komplette, integrierte Virtual Private Network- (VPN)-Lösung dar.

Routerbasierte Firewall-Funktionen

Die für eine große Palette von auf Cisco IOS-Software basierenden Routern verfügbare Cisco IOS Firewall bietet eine hochentwickelte Einhaltung von Sicherheitsregeln für Verbindungen innerhalb einer Organisation (Intranet) und zwischen Partnernetzwerken (Extranets) sowie für sichere Internetkonnektivität für Außen- und Zweigbüros.

Die Cisco IOS Firewall ist die beste Wahl für eine Integration von Multiprotokoll-Routing mit Einhaltung von Sicherheitsregeln und ermöglicht Managern die Konfiguration eines Cisco-Routers als Firewall. Kunden können die Routerplattform nach Bandbreiten-, LAN/WAN-Dichte und Multidienstanforderungen auswählen und die Vorteile erweiterter Sicherheitsmerkmale nutzen. Gehen Sie bei der Auswahl des richtigen Cisco-Routers für unterschiedliche Sicherheitsumgebungen anhand der folgenden allgemeinen Richtlinien vor:

- Kleinbüros/Heimbüros: Router der Cisco-Serien 800, UBR900, 1600 und 1720
- Zweigbüro- und Extranetumgebungen: Router der Cisco-Serien 2500, 2600 und 3600
- VPN- und WAN-Bündelungspunkte oder Umgebungen mit hohem Durchsatz: Router der Cisco-Serien 7100, 7200, 7500 und der Routen-Switch-Modul- (RSM)-Serie

Hauptvorteile

Die Cisco IOS Firewall arbeitet nahtlos mit der Cisco IOS-Software zusammen und bietet hohen Wert und außergewöhnliche Vorteile wie:

Flexibilität – Bei Installation auf einem Cisco-Router ermöglicht die skalierbare Cisco IOS Firewall-Komplettlösung Multiprotokoll-Routing, Peripheriesicherheit, Angriffserkennung, VPN-Funktionen und benutzerspezifische Authentisierung und Autorisierung.

Investitionsschutz – Durch Integration der Firewall-Funktionalität in einen Multiprotokollrouter werden vorhandene Routerinvestitionen genutzt sowie Schulungs- und Managementkosten eingespart, die mit der Einführung einer neuen Plattform verbunden sind.

VPN-Unterstützung – Die Verwendung der Cisco IOS Firewall mit den Cisco IOS-Funktionen Verschlüsselung und QoS VPN ermöglicht extrem sichere, kostengünstige Übertragungen über öffentliche Netzwerke und stellt sicher, dass der Verkehr von unternehmenskritischen Anwendungen eine hohe Zustellungspriorität erhält.

Skalierbarer Einsatz – Die für eine Vielzahl von Routerplattformen erhältliche Cisco IOS Firewall kann an alle Anforderungen an Bandbreite und Leistung eines Netzwerks angepasst werden.

Einfaches Management – Mit der Cisco ConfigMaker-Software kann ein Netzwerkadministrator die Cisco IOS-Sicherheitsfunktionen (einschließlich Cisco IOS Firewall, Netzwerkadressübersetzung und Cisco IPSec) von einer zentralen Konsole über das Netzwerk konfigurieren.

Die Cisco IOS Firewall ist auf Routern der Cisco-Serien 800, 900, 1400, 1600, 1700, 2500, 2600, 3600, 7100, 7200 und 7500 verfügbar. Darüber hinaus steht sie auf dem Catalyst[®] 5000-Switch zur Verfügung. Dieser bietet Multidienstintegration (Daten/Sprache/Video/Einwählen), fortgeschrittene Sicherheit für Einwählverbindungen und auf den 7x00-, 7500- und RSM-Serien integriertes Routing und Sicherheit am Internet-Gateway für große Unternehmen und Serviceprovider-CPE (Customer Premises Equipment).

Was gibt es Neues in der jüngsten Version? (Cisco IOS Firewall-Software 12.1(4)T)

Authentisierungs-Proxy-Abrechnung für HTTP
Abrechnung ist eine Methode zur Verfolgung der Benutzeraktionen. Abrechnungsinformationen bestehen normalerweise aus Benutzeraktion und Aktionsdauer. Die Abrechnungsinformationen werden an Abrechnungsserver gesendet, wo sie in Datensatzform gespeichert werden. Systemadministratoren verwenden diese Informationen zu Sicherheits-, Verrechnungs- oder Ressourcenzuweisungszwecke. Der Abrechnungsserver stellt Start-und-Stop-Buchführung mit genügend Informationen für ein Verrechnungs- und Sicherheits-Auditing bereit. Durch ein Hinzufügen von Authentisierung, Autorisierung und Abrechnung (AAA) zum Authentisierungs-Proxy können Kunden die Aktionen von Benutzern des Authentisierungs-Proxy-Dienstes überwachen.

Cisco Firewall-Implementierung
Wenn ein Authentisierungs-Proxy-Cache und damit verbundene dynamische Zugriffskontrolllisten (Access Control Lists, ACLs) erstellt werden, beginnt das Authentisierungs-Proxy mit der Verfolgung des Datenverkehrs vom authentisierten Host. AAA speichert Daten über dieses Ereignis. Ein Abrechnungsdatensatz oder „Startdatensatz“ kann zu diesem Zeitpunkt erzeugt werden, falls die „Start“-Option für die Abrechnung aktiviert ist. Die Firewall stellt ebenfalls einen Benutzerbefehl für die Anzeige dieser Daten bereit. Wenn ein Authentisierungs-Proxy-Cache abgelaufen ist und gelöscht wird, werden zusätzliche Daten (z. B. verstrichene Zeit) zu den Abrechnungsinformationen hinzugefügt und der „Stopdatensatz“ wird an den Server gesendet. Zu diesem Zeitpunkt werden die Informationen aus der AAA gelöscht.

Wesentliche Funktionsmerkmale der Cisco IOS Firewall

Die Cisco IOS Firewall bietet integrierte Firewall-Funktionen für Cisco-Netzwerke und verbessert die Flexibilität und Sicherheit von Cisco-Routern. Tabelle 1 gibt eine Übersicht über die wichtigsten Funktionsmerkmale.

Tabelle 1 Cisco IOS Firewall – Übersicht

Funktionsmerkmal	Beschreibung
Context-Based Access Control (CBAC)	Bietet internen Benutzern sichere, auf den einzelnen Anwendungen basierende Zugangskontrolle für allen grenzüberschreitenden Verkehr, z. B. zwischen den privaten Netzwerken von Unternehmen und dem Internet.
Angriffserkennung	Bietet Echtzeit-Überwachung, Erkennung und Reaktion auf einen Netzwerk-Missbrauch über einen breiten Satz der gängigsten Signaturen zur Angriffserkennung und Informationsgewinnung.
Authentisierungs-Proxy	Dynamische, benutzerspezifische Authentisierung und Autorisierung für LAN-basierte Verbindungen und Einwahlverbindungen; authentisiert Benutzer gegen die TACACS+ und RADIUS-Authentisierungsprotokolle des Industriestandards; ein Netzwerkadministrator kann individuelle, benutzerspezifische Sicherheitsrichtlinien festlegen.
Denial of Service-Erkennung und -Vorbeugung	Verteidigt und schützt Routerressourcen vor gebräuchlichen Angriffen; prüft Paket-Header und mustert verdächtige Pakete aus.
Dynamisches Port-Mapping	Ermöglicht einem Netzwerkadministrator, CBAC-unterstützte Anwendungen auf einem Nichtstandard-Port auszuführen.
Blockierung von Java-Applets	Schützt vor nicht identifizierten, schädlichen Java-Applets.
VPNs, IPSec-Verschlüsselung und QoS-Unterstützung	<p>Ermöglicht mit Cisco IOS-Software Verschlüsselungs-, Tunneling- und QoS-Funktionen zur Sicherung von VPNs.</p> <p>Bietet skalierbare, verschlüsselte Tunnel auf dem Router unter gleichzeitiger Integration von strenger Peripheriesicherheit, erweitertem Bandbreitenmanagement, Angriffserkennung und Service-Level-Validation.</p> <p>Standardsbasiert zur Sicherstellung von Interoperabilität</p>
Echtzeitwarnungen	Protokolliert Warnungen im Fall von Denial-of-Service-Angriffen oder anderen vorkonfigurierten Situationen; jetzt anwendungs- und funktionspezifisch konfigurierbar.
Audit Trail	Detaillierte Speicherung von Transaktionen; verzeichnet Zeitstempel, Ursprungs-Host, Ziel-Host, Ports, Dauer und Gesamtzahl von übertragenen Byte; jetzt anwendungs- und funktionspezifisch konfigurierbar.
Ereignisprotokollierung	Erlaubt Administratoren, potentielle Sicherheitslöcher oder andere nicht reguläre Aktivitäten in Echtzeit zu erkennen, indem Benachrichtigungen zu Systemfehlern über ein Konsolenterminal oder einen Syslog-Server protokolliert und ausgegeben, die Schwere des Verstoßes festgestellt und andere Parameter aufgezeichnet werden.
Firewall-Management	Ein auf Assistenten basierendes Netzwerkkonfigurations-Tool führt Schritt für Schritt durch das Netzwerkdesign, die Adressierung und die Konfiguration der Cisco IOS Firewall-Sicherheitsrichtlinie; verfügbar für Cisco 1600-, 1720-, 2500-, 2600- und 3600-Router; unterstützt auch NAT- und IPSec-Konfigurationen.
Integration mit Cisco IOS-Software	Arbeitet mit den Cisco IOS-Funktionen bei der Integration der Einhaltung von Sicherheitsrichtlinien in das Netzwerk zusammen.
Elementare und erweiterte Filterung des Datenverkehrs	<p>Standard- und erweiterte Zugriffskontrolllisten (Access Control Lists, ACLs) – Wenden Zugriffskontrollen auf spezielle Netzwerksegmente an und bestimmen, welche Daten durch ein Netzwerksegment passieren dürfen.</p> <p>Schloss und Schlüssel – Dynamische ACLs gewähren nach Benutzeridentifikation temporären Zugang durch die Firewalls (Benutzername/Kennwort).</p>
Unterstützung für mehrere Schnittstellen auf Richtlinienbasis	Ermöglicht die Kontrolle des Benutzerzugriffs nach IP-Adresse und Schnittstelle gemäß der Sicherheitsrichtlinie.
Redundanz/Failover	Bei einem Ausfall wird der Verkehr automatisch zu einem Backup-Router geroutet.
Übersetzung von Netzwerkadressen (Network Address Translation, NAT)	Versteckt das interne Netzwerk für erweiterte Sicherheit vor dem externen.
Zeitspezifische Zugriffslisten	Definieren die Sicherheitsrichtlinie nach Tageszeit und Wochentag
Peer-Router-Authentisierung	Stellt sicher, dass Router zuverlässige Routinginformationen von vertrauenswürdigen Quellen erhalten.

Funktionsmerkmal	Beschreibung
Verbesserte Angriffserkennung und Verteidigung für E-Mail-Server	Neue Angriffserkennung wurde besonders für SMTP-orientierte Angriffe entworfen.

Context-Based Access Control (CBAC)

Die Cisco IOS Firewall CBAC-Engine bietet sichere, anwendungsspezifische Zugriffskontrolle über die Netzwerkperipherie. Sie erhöht durch Untersuchung der Ursprungs- und der Zieladressen die Sicherheit von TCP- und UDP-Anwendungen (User Datagram Protocol), die bekannte Ports verwenden (wie etwa FTP- und E-Mail-Daten). CBAC ermöglicht einem Netzwerkadministrator die Implementierung von Firewall-Intelligenz als Teil einer integrierten Single-Box-Lösung.

Bei Sitzungen mit einem Extranetpartner unter Verwendung von Internet- oder Multimedia-Anwendungen oder Oracle-Datenbanken zum Beispiel ist das Öffnen eines Network-Doorway, der über Schwächen im Netzwerk des Partners zugänglich ist, nicht mehr erforderlich. Mit CBAC können stark gesicherte Netzwerke den grundlegenden Anwendungsverkehr von heute sowie erweiterte Anwendungen wie Multimedia und Videokonferenz sicher über einen Router ablaufen lassen.

Die Auswirkungen von CBAC auf die Netzwerksicherheit

CBAC ist ein anwendungsbezogener Kontrollmechanismus für IP-Datenverkehr, der Standard-TCP- und UDP-Internetanwendungen, Multimedia-Anwendungen (H.323- und andere Videoanwendungen) sowie Oracle-Datenbanken einschließt. CBAC untersucht TCP- und UDP-Pakete und protokolliert ihren Zustand oder Verbindungsstatus.

TCP ist ein verbindungsorientiertes Protokoll. Vor der Datenübertragung handelt ein Ursprungs-Host mit der Zieladresse eine Verbindung aus; dieser Vorgang ist als „Three-Way Handshake“ bekannt. Dieser Vorgang, bei dem die Verbindungsparameter ausgehandelt werden, gewährleistet gültige TCP-Verbindungen und fehlerfreie Übertragungen. Während des Verbindungsaufbaus durchläuft TCP verschiedene Zustände oder Phasen, die anhand der Paket-Header leicht zu identifizieren sind. Standardmäßige sowie erweiterte ACLs lesen den Zustand aus dem Paket-Header und bestimmen, ob der Datenverkehr über eine Verbindung zugelassen ist.

CBAC liest das gesamte Paket, um Informationen über den Anwendungsstatus zu erhalten, und erweitert so die ACL-Funktionsmerkmale um Untersuchungsfunktionen. Unter Verwendung dieser Informationen erstellt CBAC einen temporären, sitzungsbezogenen ACL-Eintrag und ermöglicht dadurch Datenverkehr zurück in das „vertrauenswürdige“ Netzwerk. Diese temporäre ACL öffnet also eine „Tür“ in der Firewall. Wenn eine Sitzung aufgrund einer Zeitüberschreitung abgebrochen oder beendet wird, wird der ACL-Eintrag gelöscht und die Tür für weiteren Datenverkehr geschlossen. Standardmäßige und erweiterte ACLs können keine temporären ACL-Einträge erstellen, so dass Administratoren bisher gezwungen waren, die Sicherheitsrisiken gegen die Anforderungen an den Zugang zu Informationen abzuwägen. Weiterentwickelte Anwendungen, die für die Rückübertragung von Daten unter mehreren Kanälen auswählen, sind unter alleiniger Verwendung standardmäßiger oder erweiterter ACLs schwer abzusichern.

CBAC ist sicherer als die gegenwärtigen rein ACL-basierten Lösungen, da für die Entscheidung, ob eine Sitzung Daten durch die Firewall übertragen kann, der Anwendungstyp berücksichtigt und festgestellt wird, ob dieser Typ für die Rückübertragung von Daten unter mehreren Kanälen auswählt. Vor der Einführung von CBAC konnten Administratoren die Datenübertragung durch hoch entwickelte Anwendungen nur zulassen, indem sie permanente ACLs eintrugen, welche im Wesentlichen die „Firewall-Türen“ offen hielten, so dass die meisten Administratoren sich dafür entschieden, solche Datenübertragungen gar nicht erst zuzulassen. Mit CBAC können sie jetzt Datenübertragungen von Multimedia- und anderen Anwendungen ohne Risiko zulassen, indem sie die Firewall bei Bedarf öffnen und ansonsten geschlossen halten. Ist CBAC z. B. so konfiguriert, dass Microsoft NetMeeting zugelassen wird, wenn ein interner Benutzer eine Verbindung einleitet, dann erlaubt die Firewall Rückverkehr zum internen Benutzer. Wenn aber eine externe NetMeeting-Quelle eine Verbindung mit einem internen Benutzer initiiert, unterbindet CBAC den Zugang und verwirft das Paket.

Angriffserkennung

Intrusion Detection Systems (IDS) bieten einen Schutz, der über die Firewall hinausgeht, indem das Netzwerk vor internen und externen Angriffen und Gefahren geschützt wird. Die Cisco IOS Firewall IDS-Technik verbessert den Peripherie-Firewall-Schutz durch die Ergreifung entsprechender Maßnahmen für Pakete und Flüsse, die die Sicherheitsrichtlinien brechen oder eine gefährliche Netzwerkaktivität darstellen.

Die Fähigkeiten der Cisco IOS Firewall Angriffserkennung eignen sich ideal für zusätzliche Einsichtnahme bei Intranet, Extranet und Zweigbüro-Internetperipherie. Netzwerkadministratoren erhalten jetzt einen noch wirkungsvolleren Schutz gegen Angriffe auf das Netzwerk und können auf Gefahren von internen oder externen Hosts automatisch reagieren.

Erkennung und Reaktion

Die IDS der Cisco IOS Firewall identifiziert 59 der gängigsten Angriffe. Dabei verwendet sie Signaturen, um Missbrauchsmuster im Netzwerkverkehr aufzudecken. Die Signaturen zur Angriffserkennung in der neusten Version von Cisco IOS Firewall wurden aus einem breiten Querschnitt von Signaturen zur Angriffserkennung ausgewählt. Sie repräsentieren schwere Sicherheitsverletzungen und die meisten gängigen Netzwerkangriffe und Scans zur Informationsgewinnung.

Die Cisco IOS Firewall arbeitet als Inline-Sensor für Angriffserkennung. Sie überwacht Pakete und Sitzungen bei ihrem Durchgang durch den Router und scannt diese auf Übereinstimmung mit einer der IDS-Signaturen. Wird eine zweifelhafte Aktivität entdeckt, reagiert sie, bevor die Netzwerksicherheit gefährdet werden kann, und registriert das Ereignis über Cisco IOS-Syslog. Der Netzwerkadministrator kann das IDS-System so konfigurieren, dass eine entsprechende Reaktion auf unterschiedliche Gefahren erfolgt. Sobald Pakete einer Sitzung mit einer Signatur übereinstimmen, kann das IDS-System auf folgende Reaktionen konfiguriert werden:

Senden eines Alarms an einen Syslog-Server oder ein Cisco Secure Intrusion Detection System (wurde früher als das NetRanger[®]-System bezeichnet)

- Director (zentralisierte Managementschnittstelle)
- Verwerfen des Pakets
- Rücksetzen der TCP-Verbindung

Cisco entwickelte die auf der IOS-Software basierenden Fähigkeiten zur Angriffserkennung der Cisco IOS Firewall mit Blick auf Flexibilität, so dass bei falschen Positivmeldungen einzelne Signaturen ausgeschaltet werden können. Obwohl vorzugsweise beide Funktionen der CBAC-Sicherheits-Engine, die Firewall und die Angriffserkennung zur Einhaltung der Sicherheitsrichtlinien aktiviert sein sollten, kann jede dieser Funktionen unabhängig und auf unterschiedlichen Routerschnittstellen ausgeschaltet werden. Die auf der Cisco IOS-Software basierende Angriffserkennung ist Teil der Cisco IOS Firewall und verfügbar auf Routern der Cisco-Serien 1720, 2600, 3600, 7100, 7200, 7500 und dem RSM für Catalyst 5000-Switches. Sämtliche Plattformen mit der Cisco IOS Firewall erkennen fünf der häufigsten SMTP-Angriffe.

Cisco Secure: Integrierte Software und Intrusion Detection System

Die Kunden des Cisco Secure Intrusion Detection System können die auf der Cisco IOS-Software basierenden IDS-Signaturen einsetzen, um ihre vorhandenen IDS-Systeme zu ergänzen. Dies ermöglicht den Einsatz von IDS in Bereichen, die eventuell einen NetRanger-Sensor nicht unterstützen können. Cisco IOS IDS-Signaturen können zusammen oder unabhängig von den Cisco IOS Firewall-Funktionen eingesetzt werden.

Die Cisco IOS Firewall mit Angriffserkennung kann dem Cisco Secure IDS Director-Bildschirm als Symbol hinzugefügt werden, um einen umfassenden Überblick über alle Sensoren zur Angriffserkennung in einem Netzwerk zu bieten. Die Cisco IOS Firewall-Funktionen zur Angriffserkennung verfügen über einen erweiterten Berichtsmechanismus, der eine Aufzeichnung bei der Cisco Secure IDS Director-Konsole zusätzlich zum Cisco IOS-Syslog ermöglicht.

Authentisierungs-Proxy

Ein Netzwerkadministrator kann mit der LAN-basierten, dynamischen, benutzerspezifischen Authentisierung und Autorisierung der Cisco IOS Firewall für jeden Benutzer spezifische Sicherheitsrichtlinien erstellen. Bisher erfolgten die Identifizierung eines Benutzers und die zugehörige Zugriffsautorisierung über die feste IP-Adresse eines Benutzers, oder es musste eine einzelne Sicherheitsrichtlinie für eine ganze Benutzergruppe oder ein Subnetz angewendet werden. Jetzt können benutzerspezifische

Richtlinien dynamisch von einem TACACS+ oder RADIUS- Authentisierungs-Server unter Verwendung der Authentisierungs-, Autorisierungs- und Abrechnungsdienste (AAA) der Cisco IOS-Software in den Router geladen werden.

Ein Benutzer kann sich beim Netzwerk oder Internet über HTTP anmelden und sein spezifisches Zugriffsprofil wird automatisch geladen. Entsprechende dynamische und individuelle Zugriffsprivilegien stehen bei Bedarf zur Verfügung und schützen das Netzwerk gegenüber einer allgemeineren Richtlinie, die für mehrere Benutzer angewendet wird. Authentisierung und Autorisierung können auf jede Richtung der Routerschnittstelle angewendet werden und sichern so den Eingang und Ausgang bei Extranet-, Intranet- und Internetnutzung.

Denial of Service-Erkennung und -Vorbeugung

Erweiterte Denial of Service-Erkennung und -Vorbeugung verteidigen das Netzwerk gegen Angriffe nach dem SYN-Flooding-Schema (synchronize/start), Port-Scans und Paket-Injektion durch Überprüfung der Paket-Sequenznummern bei TCP-Verbindungen. Wenn die Nummern nicht innerhalb eines erwarteten Bereichs liegen, verwirft der Router verdächtige Pakete. Erkennt der Router eine ungewöhnlich hohe Rate neuer Verbindungen, gibt er eine Alarmmeldung ab und verwirft darüber hinaus halboffene TCP-Verbindungszustandstabellen, um eine Erschöpfung von Systemressourcen zu verhindern.

Entdeckt die Cisco IOS Firewall einen möglichen Angriff, verfolgt sie den Benutzerzugriff über Quell- oder Zieladresse und Portpaare. Sie detailliert außerdem die Transaktion und erstellt ein Audit Trail.

Dynamisches Port-Mapping

Flexibles, anwendungsspezifisches Port-Mapping ermöglicht CBAC-gestützten Anwendungen den Ablauf auf einem Nichtstandard-Port. Diese Funktion ermöglicht es einem Netzwerkadministrator, die Zugriffskontrolle für spezielle Anwendungen und Dienste anzupassen, um die unterschiedlichen Anforderungen eines Netzwerks zu erfüllen.

Blockierung von Java-Applets

Mit der starken Zunahme an Java-Applets aus dem Internet ist der Schutz von Netzwerken vor bösartigen Applets nun ein Hauptanliegen von Netzwerkmanagern. Java-

Blockierung kann so konfiguriert werden, dass der Zugang zu kleinen Java-Anwendungen, die nicht in einem Archiv oder einer komprimierten Datei eingebaut sind, gefiltert oder vollständig verwehrt werden kann.

VPN, IPSec-Verschlüsselung und QoS-Unterstützung

In Kombination mit der Cisco IPSec-Technik bietet die Cisco IOS Firewall integrierte VPN-Funktionalität. VPNs werden schnell weiterentwickelt, um eine sichere Datenübertragung über öffentliche Leitungen (wie etwa das Internet) zu bieten, die Implementierungs- und Managementkosten für Fernbüros und Extranets zu senken und Quality of Service (QoS) und Zuverlässigkeit zu erweitern.

Die Cisco IOS Firewall arbeitet bei der Sicherung von VPNs mit Verschlüsselungs-, Tunneling- und QoS-Funktionen der Cisco IOS-Software. Die Verschlüsselungsfunktion auf Netzwerkebene verhindert Abhören und Manipulation von Daten während der Übertragung im gesamten Netzwerk. Die Cisco IOS Firewall verschlüsselt Daten für private Kommunikationen über nicht sichere Netzwerke unter Verwendung von Internet Protocol Security (IPSec) mit 56-Bit- (DES) und 168-Bit- (3DES)-Verschlüsselungstechnik.

Für maximale Interoperabilität unterstützt die Cisco IOS-Software mehrere Tunneling-Protokollstandards und arbeitet mit Generic Routing Encapsulation (GRE), Layer 2 Forwarding (L2F) und Layer 2 Tunneling Protocol (L2TP). QoS-Funktionen klassifizieren den Verkehr, managen Überlastungen und bevorzugen Anwendungen bei Bedarf.

Die Cisco IOS Firewall kann zusammen mit Cisco-VPN-fertigen Plattformen, insbesondere den Routern der Cisco-Serien 1720, 2600, 3600 und 7100 eingesetzt werden, die ein bestehendes Netzwerk auf Virtual Private Networking erweitern. Cisco weiß, dass VPN-Lösungen mehr als sichere, verschlüsselte Tunnel über öffentliche Netzwerkeinrichtungen bieten müssen. Sie müssen auch eine rechtzeitige und zuverlässige Zustellung von Daten sicherstellen und robuste Peripheriesicherheit für das Unternehmens-Portal zum öffentlichen Netzwerk ermöglichen. Die Cisco IOS Firewall bietet in Kombination mit beispielsweise einem Router der 7100-Serie skalierbare, verschlüsselte Tunnel unter gleichzeitiger Integration von strenger Peripheriesicherheit, erweitertem Bandbreitenmanagement, Angriffserkennung und Service-Level-Validation.

Die Funktion Authentisierungs-Proxy der Cisco IOS Firewall bietet ebenfalls Benutzerauthentisierung und -autorisierung für Cisco VPN Client-Software.

Konfigurierbare Echtzeitalarme, Audit Trails und Ereignisprotokollierung

Echtzeitwarnungen erfolgen in Form von Syslog-Fehlermeldungen an zentrale Managementkonsolen, wenn verdächtige Aktivitäten entdeckt werden, so dass Netzwerkmanager sofort auf Eindringlinge reagieren können. Verbesserte Leistungsmerkmale verwenden Syslog, um alle Transaktionen zu protokollieren, wobei Datum/Uhrzeit, Ursprungs-Host, Ziel-Host, verwendete Ports, Sitzungsdauer und die Gesamtzahl der übertragenen Byte aufgezeichnet werden.

Die Cisco IOS Firewall-Funktionen zu Alarm und Audit Trail sind nun konfigurierbar, wodurch eine flexiblere Berichterstattung und Fehlerverfolgung möglich wird. Die konfigurierbaren Funktionen zum Audit Trail unterstützen modulare Verfolgung spezieller CBAC-gestützter Anwendungen und Java-Blockierung. Die Funktionen zu Echtzeitalarm und Audit Trail werden durch eine Vielzahl von Berichtstools von Drittanbietern unterstützt.

Sobald eine Störung des Netzwerks auftritt, wird über den Syslog-Mechanismus der Cisco IOS-Software eine Alarmmeldung für den Berichts-Host erstellt. Dies erlaubt Administratoren, potentielle Sicherheitslöcher oder andere nicht reguläre Aktivitäten in Echtzeit zu erkennen, indem Benachrichtigungen zu Systemfehlern über ein Konsolenterminal oder einen Syslog-Server protokolliert und ausgegeben, die Schwere des Verstoßes festgestellt und andere Parameter aufgezeichnet werden.

Firewall-Management

Die Umsetzung von Sicherheitsrichtlinien und das Management der Cisco IOS Firewall können schnell und einfach mit dem GUI-basierten Management von einem zentralen Ort aus durchgeführt werden. Cisco ConfigMaker 2.1 und höhere Versionen verfügen über einen Sicherheits-Assistenten für eine schrittweise Anleitung bei der schnellen Konfiguration einer Sicherheitsrichtlinie für die Cisco IOS Firewall. Sie unterstützen ebenfalls NAT- und IPSec-Konfiguration.

ConfigMaker ist ein benutzerfreundliches Microsoft Windows 95-, Windows 98- und Windows NT 4.0-Programm, das für die Konfiguration eines kleinen Netzwerks von Cisco-Routern, -Switches, -Hubs und anderen Netzwerkgeräten von einem einzigen PC aus entwickelt wurde. Es ist für die Router der Cisco-Serien 800, 1600, 1720, 2500, 2600 und 3600 verfügbar.

Integration mit Cisco IOS-Software

Die Cisco IOS Firewall ist eine Sicherheitslösung, die über die Cisco IOS-Software zu einem Bestandteil des Netzwerks wird. Zu einer leistungsfähigen Sicherheitsrichtlinie gehört mehr als Peripheriekontrolle oder Firewall-Setup und -Management – die Einhaltung von Sicherheitsrichtlinien muss ein eigener Bestandteil des Netzwerks sein. Die Cisco IOS-Software ist ein ideales Instrument für die Implementierung globaler Sicherheitsrichtlinien. Der Aufbau einer durchgängigen Cisco-Lösung versetzt Manager in die Lage, Sicherheitsrichtlinien für das gesamte Netzwerk durchzusetzen, während es sich im Ausbau befindet.

Die Cisco IOS Firewall bietet komplette Interoperabilität mit den Funktionen der Cisco IOS-Software, einschließlich NAT, VPN-Tunneling-Protokollen, Cisco Express Forwarding (CEF), AAA-Erweiterungen, Cisco Verschlüsselungstechnik und Cisco IOS IPsec.

Wer sollte die Cisco IOS Firewall verwenden?

- Kunden, die eine One-Box-Lösung mit leistungsfähigen Funktionen zu Sicherheit, Angriffserkennung, benutzerspezifischer Authentisierung und Autorisierung, VPN-Funktionen und Multiprotokoll-Routing benötigen
- Kunden, die an einer kostengünstigen Methode zur Erweiterung der Peripheriesicherheit über die Grenzen des Netzwerks hinaus interessiert sind, insbesondere Zweigbüro-, Intranet- und Extranetperipherie
- Klein- und Mittelbetriebe, die einen preisgünstigen Router mit integrierter Firewall und Angriffserkennung suchen

- Kunden von Dienst Anbietern, die einen Einsatz als Router/Firewall-Paket für gemanagte Dienste planen
- Kunden, die zusätzliche Sicherheit zwischen Netzwerksegmenten benötigen (wie zwischen ihren Organisationen und einem weniger vertrauenswürdigen Partnerstandort)
- Organisationen mit Intranetanschlüssen, bei denen zusätzliche Sicherheit unabdingbar ist
- Zweigbüros, die an einen Unternehmenssitz oder das Internet angeschlossen sind
- Kunden, die bereits Cisco IOS besitzen und keine getrennte Firewall-Plattform wünschen
- Kunden, die Firewall-Schutz in einer Netzwerkstruktur einrichten möchten, um eine starke Verteidigungsumgebung zu schaffen



Unternehmenszentrale
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Telefon: +1 408 526 4000
+1 800 553 NETS (6387)
Fax: +1 408 526 4100

Zentrale Europa
Cisco Systems Europe
11, Rue Camille Desmoulins
92782 Issy Les Moulineaux
Cedex 9
Frankreich
www.cisco.com
Telefon: +33 1 58 04 60 00
Fax: +33 1 58 04 61 00

Zentrale Amerika
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Telefon: +1 408 526 7660
Fax: +1 408 527 0883

Zentrale Asien/Pazifik
Cisco Systems Australia, Pty., Ltd
Level 17, 99 Walker Street
North Sydney
NSW 2059 Australien
www.cisco.com
Telefon: +61 2 8448 7100
Fax: +61 2 9957 4350

Cisco Systems ist mit mehr als 190 Niederlassungen in den folgenden Ländern vertreten. Adressen, Telefon- und Faxnummern finden Sie auf der Cisco.com-Website unter www.cisco.com/go/offices.

Argentinien • Australien • Belgien • Brasilien • Chile • China • Costa-Rica • Dänemark • Deutschland • Dubai, VAE • Finnland • Frankreich • Griechenland
Hongkong • Indien • Indonesien • Irland • Israel • Italien • Japan • Kanada • Kolumbien • Korea • Kroatien • Luxemburg • Malaysia • Mexiko • Neuseeland
Niederlande • Norwegen • Österreich • Peru • Philippinen • Polen • Portugal • Puerto-Rico • Rumänien • Russland • Saudi-Arabien • Schweden • Schweiz • Singapur
Slowakei • Slowenien • Spanien • Südafrika • Taiwan • Thailand • Tschechische Republik • Türkei • Ukraine • Ungarn • USA • Venezuela • Vereinigtes Königreich

Copyright © 2000, Cisco Systems, Inc. Alle Rechte vorbehalten. Gedruckt in den USA. Catalyst, Cisco, Cisco IOS, Cisco Systems, das Cisco Systems-Logo und NetRanger sind eingetragene Marken von Cisco Systems, Inc. in den USA und bestimmten anderen Ländern. Alle anderen in diesem Dokument erwähnten Marken sind das Eigentum der jeweiligen Besitzer. Die Verwendung des Wortes „Partner“ impliziert keine Partnerschaftvereinbarung zwischen Cisco und einer anderen Firma. (0007R) 9/00 LW

Wie sieht es mit dem Support von Cisco aus?

Zusätzlich zu seinen führenden Netzwerklösungen ist Cisco Systems für seine durchgängigen Supportlösungen von Weltklasse bekannt, die Netzwerkmanager bei Cisco-LAN- oder -WAN-Netzwerken unterstützen.

Ciscos Support-Produktportfolio umfasst Inbetriebnahme, Wartung, Marketing und hochentwickelte, kundenspezifische Dienstleistungen, um Ihre Investitionen zu maximieren und zu schützen. Aktualisierungen der Cisco IOS Firewall-Software sind jederzeit über Cisco Connection Online (CCO), der prämierten Cisco-Website, erhältlich.

Verfügbarkeit und Preise

Die Cisco IOS Firewall steht als Softwareimage-Option für die Router der Cisco-Serien 800, UBR900, 1600, 1720, 2500, 2600, 3600, 7100, 7200 und 7500 zur Verfügung. Sie können das Softwareimage von der Cisco-Website laden oder es auf CD-ROM anfordern. Preisinformationen erhalten Sie von Ihrer Cisco-Niederlassung bzw. Ihrem Cisco-Händler oder auf der Cisco-Website unter <http://www.cisco.com>.

Weitere Informationen

Weitere Informationen über die Cisco IOS- und Cisco Secure Integrated-Software finden Sie auf der Cisco-Website unter www.cisco.com/warp/public/cc/cisco/mkt/security/index.shtml.