Microsoft®
Internet Security & Acceleration Server 2004

Übersicht zur Beta 2

Jochen Sommer
Senior Presales Consultant, MCSE, MCT
Microsoft Deutschland GmbH

Agenda

- Die Zielsetzung von Microsoft
- Aktuelle Sicherheitssituation
- Auswirkungen für Kunden
- Produktübersicht
- Fortgeschrittene Schutzmechanismen
- Einfache Bedienung
- Hohe Performance
- Zusammenfassung

Die Zielsetzung von Microsoft

"Sicherheit hat die höchste Priorität für Microsoft. Wir unterstützen unsere Kunden dabei, ihr geistiges Eigentum und Ihre Daten zu schützen."

Security is a top priority for Microsoft, and we are committed to helping our customers protect their intellectual property and data

- Remediation (Heilen)
- Innovation

Aktuelle Sicherheitssituation

Von 2000 bis 2002 stiegen die gemeldeten Störungen (Incidents) von 21,756 auf 82,094 – CERT, 2003

80 % von 445 befragten Personen gaben an, dass das Internet ein ständiger Angriffspunkt sei. Vier Jahre früher waren es nur 57%.

– CSI/FBI Computer Crime and Security Survey

Ungefähr 70 Prozent aller Attacken aus dem Internet finden auf Applikationsebene statt

- Gartner

Auswirkungen für Kunden

Angriffe auf Applikationsebene:

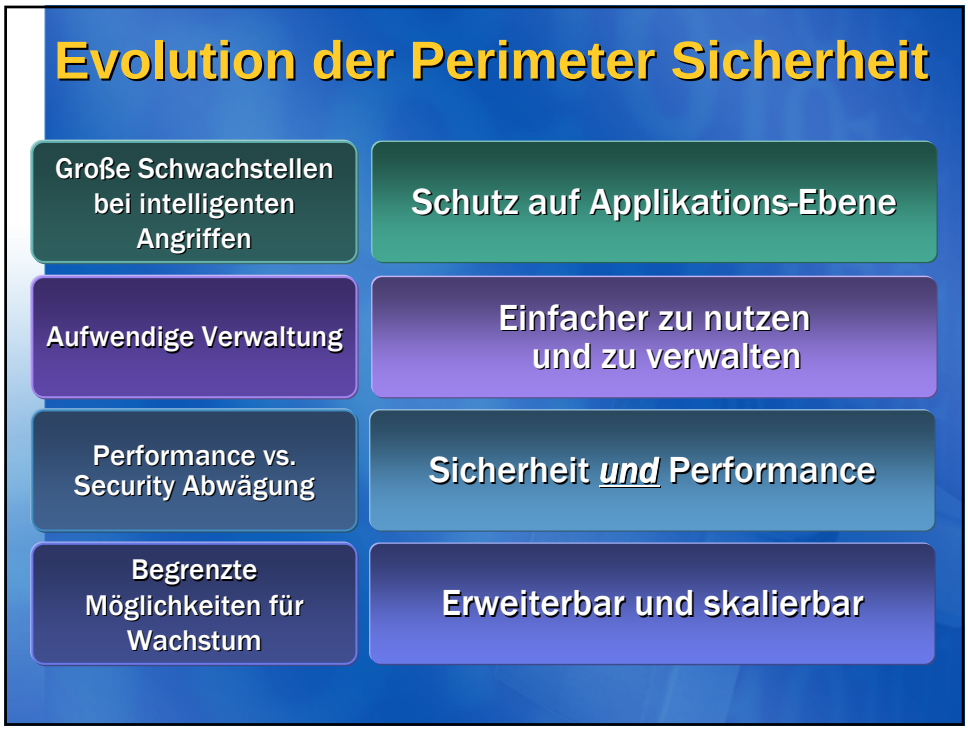
- Identitätsdiebstahl
- Veränderung von Webseiten
- Unautorisierter Zugriff
- Veränderung von Daten, Protokollen und Aufzeichnungen
- Diebstahl von Informationen
- Unterbrechung von Diensten

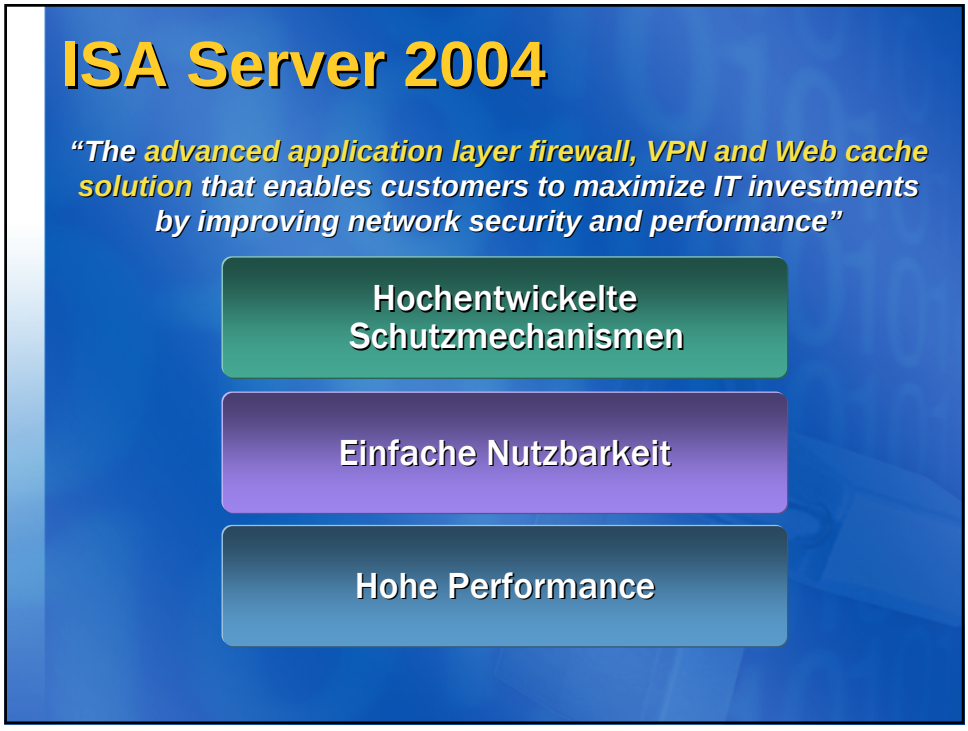
Implikationen:

- Finanzielle Verluste
- Vertrauen / Image
- Juristische Konsequenzen
- Tauschbörsen
- Produktpiraterie
- Personalangelegenheiten
- Ansprüche von Aktionären
- Ansprüche von Kunden
- Ansprüche von Partnern

Traditionelle Firewalls

Große Schwachstellen bei intelligenten Angriffen	▪ Intrusions ▪ SSL-basierte Angriffe
Aufwendige Verwaltung	▪ Sicherheit ist ein komplexes Thema ▪ IT-Abteilung ist bereits überlastet
Performance vs. Security Abwägung	▪ Hochperformante Systeme sind zu teuer ▪ Komplexes Design - schwierige Administration
Begrenzte Möglichkeiten für Wachstum	▪ Kein einfacher Upgrade-Pfad ▪ Skaliert nicht mit Business-Anforderungen


Evolution der Perimeter Sicherheit
Große Schwachstellen bei intelligenten Angriffen
Schutz auf Applikations-Ebene
Aufwendige Verwaltung
Einfacher zu nutzen und zu verwalten
Performance vs. Security Abwägung
Sicherheit und Performance
Begrenzte Möglichkeiten für Wachstum
Erweiterbar und skalierbar


ISA Server 2004
"The advanced application layer firewall, VPN and Web cache solution that enables customers to maximize IT investments by improving network security and performance"
Hochentwickelte Schutzmechanismen
Einfache Nutzbarkeit
Hohe Performance

Einsatzszenarien:

- Grenz-Firewall
  - Caching
  - Chaining
- Sichere Veröffentlichung
  - Exchange Server
  - Web-Server
- Remote Access (VPN)
- Anbindung von Niederlassungen
  - Remote site security
  - Site-to-Site VPN (IPSec)
- Integrierte Lösung
  - Ein-Server Sicherheits-lösung für Perimeter
  - Einfaches, vereinheit-lichtes Management
- Flexible Topologien
  - 3-Leg, Front/Back, ...
  - Schutz einzelner Komponenten
  - Multi-Netzwerk-Support
  - Partitionierung

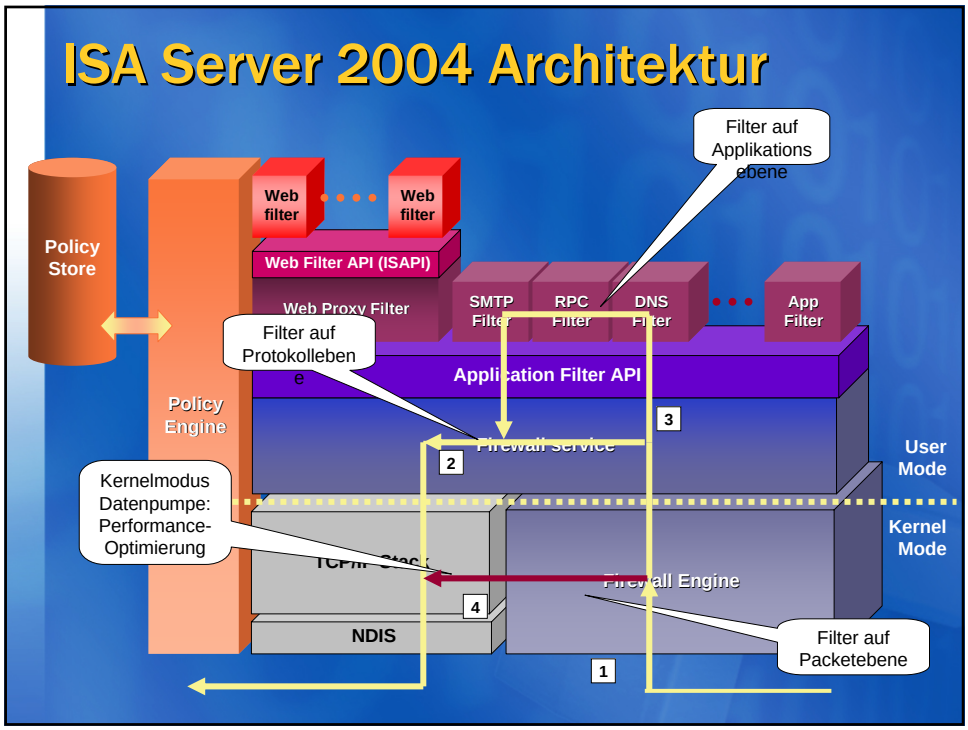
ISA Server 2004 Neue Features

Aktualisierte Sicherheits-Architektur

Hochentwickelte Schutzmechanismen

Sicherheit auf Applikations-Ebene, entwickelt um Microsoft Applikationen optimal zu schützen

Deep Content Inspection	• Erweiterte HTTP- und anpassbare Prot-Filter • Umfassende und flexible Richtlinien • Stateful routing
Optimierte Exchange Server Integration	• Support für Outlook “RPC over HTTP(s)” • Erweiterte Outlook Web Access Security • Leichte Konfiguration über Assistenten
Vollständig integrierte VPN Lösung	• Vereinheitlichte Firewall-VPN Filterung • Unterstützung für site-to-site IPsec™ • Integration mit Windows Quarantine
Umfassende Authentifizierung	• Unterstützung von RADIUS und RSA SecurID • Benutzer- und Gruppenbasierende Richtlinien • Erweiterbar durch Drittanbieter-Tools



Filterung auf Applikations-Ebene

- Aktuelle Angriffsszenarien erfordern Filterung auf Applikations-Ebene
  - Schützt Netzwerkkomponenten vor Schwachstellen auf Applikations-Ebene
  - Stellt die Möglichkeit bereit, eine detaillierte und granulare Sicherheitsrichtlinie auf Applikationsebene zu definieren
  - Bester Schutz für Microsoft Applikationen
- Applikations-Filter Framework
  - Integrierte Filter für gängige Protokolle:
    - HTTP, SMTP, RPC, FTP, H.323, DNS, POP3, Streaming Media
  - Szenarien-basierendes Design
  - Erweiterbare plug-in Architektur

VPN Schutzmechanismen

- "Enttunnelter" Datenverkehr wird untersucht
- VPN Datenverkehr wird beschränkt
  - VPN-Netzwerk: Adressen werden VPN-Benutzern zugewiesen
  - IP-Adressen werden dynamisch hinzugefügt/entfernt
- Support für IPSec Tunnel Mode
  - Verbindung von Zweigstellen über VPN
  - Vereinfachte Administrationstools
- Unterstützung für Netzwerk-Quarantäne
  - Quarantäne-Benutzer werden in speziellen Quarantäne-Netzwerken platziert
  - IP-Adressen werden dynamisch hinzugefügt/entfernt

Sicherheitsoptimierung der Engine

- Flood-DoS-Schutz
  - SYN-flood
  - Client-Verbindungsquota
    - anwendbar bei Worm/Virus floods
  - Vermeidung von Spoofed UDP-Packet flooding
- Attacken/Angriffs-Erkennung
  - IP-Optionen, DNS-Attacken, IP half-scan, Port scan
- IP-Optionen Filter
  - Filter basierend auf individuellen Einstellungen
- Lockdown-Modus
  - Beschränkung der Firewall bei Service-Fehlern

Authentifizierungs Framework

- Authentifikation
  - Firewallclient-Authentifizierung
    - Transparente Benutzerauthentifikation
      - LSP wird im Benutzerkontext geladen
      - applikationstransparent, protokollunabhängig
    - Kerberos/NTLM
  - Web proxy-Authentifizierung
    - Proxy-Auth, Reverse proxy-Auth, Pass through-Auth, SSL bridging
    - Basic, digest, NTLM, Kerberos, Certificates
    - RADIUS-Auth., SecurID-Auth.
    - CRL Unterstützung
    - Erweiterbar!
  - VPN-Clients
    - EAP (Zertifikate, Smartcards, etc.), MS-CHAPv2, CHAP, (S-PAP, PAP)
    - RADIUS / Windows
- Erweiterbare Authentifizierung "Authorization framework"
  - Filter von Drittanbietern können eigene Namespaces registrieren

ISA Server 2004 New Features

Neue Management-Werkzeuge und Benutzeroberfläche

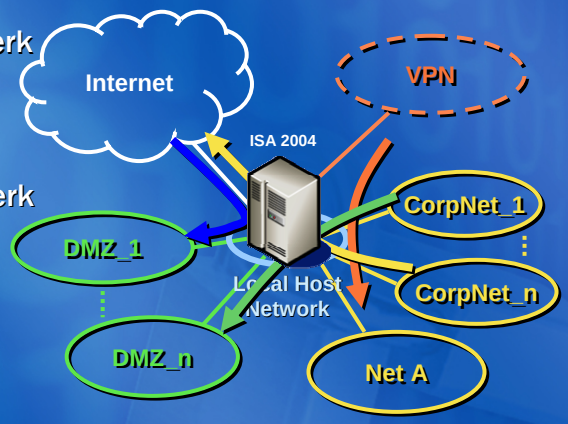
Ease of Use

Effiziente und kosteneffektive Lösung für Netzwerksicherheit

Multi-Netzwerk Architektur	• Unlimitierte Netzwerkdefinitionen und -typen • Firewall-Richtlinien werden auf • jeden Datenverkehr angewendet
Netzwerk-Vorlagen und Assistenten	• Assistant automatisiert Netzwerkrouting • Unterstützung von fünf Standardtopologien • Beliebig anpassbar für alle Szenarien
Grafischer Editor für Richtlinien	• Einheitl. Firewall/VPN Richtlinien • Drag/drop mit szenariobasierten Assistenten • XML-basierender Konfigurationsexport/import
Optimierte Analysemöglichkeiten	• Vollständig neues Monitoring-Dashboard • Echtzeitviewer für Log-Dateien

ISA 2004 Netzwerk-Modell

- Beliebige Anzahl Netzwerke
- VPNs als Netzwerk
- Localhost als Netzwerk
- Zugeordnete Beziehungen (NAT / Route)
- Richtlinie pro Netzwerk
- Paketfilterung auf allen Interfaces
- *Jede Topologie - jede Richtlinie!*



Netzwerk-Vorlagen

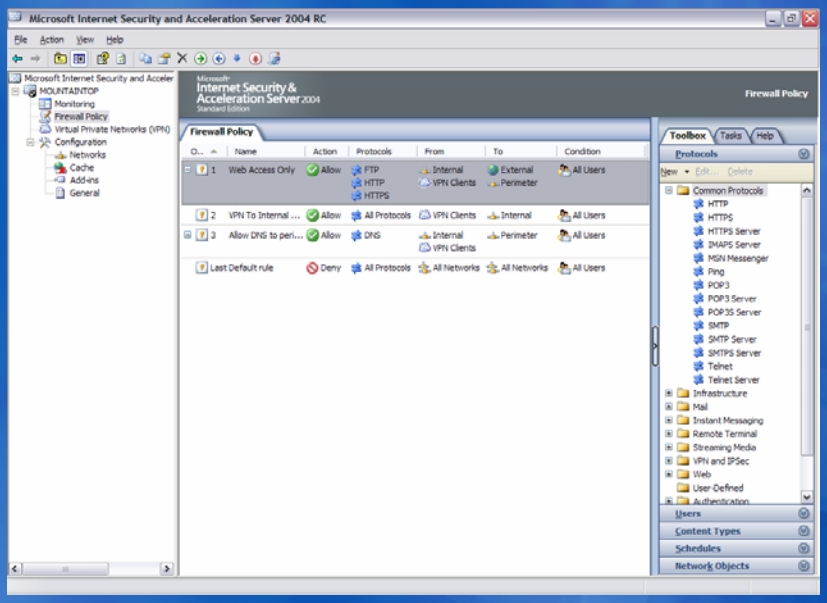
Zielsetzung
- Einfache Netzwerk-Verwaltung

Features
- Fünf Vorlagen
- Automatische Routingbeziehungen
- Anpassbar

ISA Server 2004 Richtlinien-Modell

- Einheitliches und sortiertes Regelwerk
  - Logischer Aufbau und einfacher zu verstehen
  - Einfachere Ansicht und Kontrolle
- Neue und vereinheitlichte Regelstruktur
  - Anwendbar auf jeden Richtlinientyp
  - Drei grundlegende Klassen von Regeln
    - Zugriffsregeln
    - Regeln zur Server-Veröffentlichung
    - Web-Veröffentlichungsregeln
  - Die Eigenschaften der Filterung auf Applikations-Ebene ist ein Bestandteil der jeweiligen Regel
- Standardsystemrichtlinie

Grafischer Editor für Richtlinien



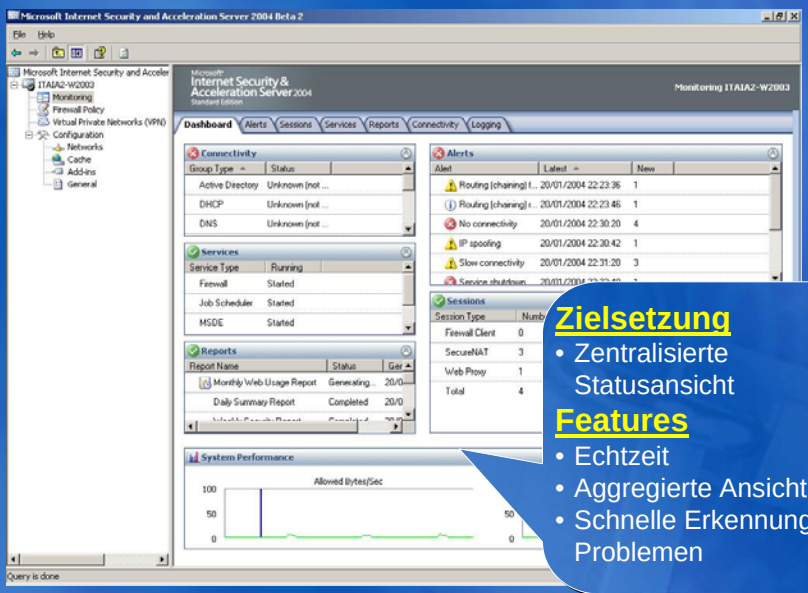
ISA Server 2004 Monitoring

- Zielsetzung
  - Server Status – Kritischer Service im Netzwerk
  - Troubleshooting – Schnelle und einfache Analyse
  - Unterschungen – Angriffe, Fehlkonfigurationen
  - Planungsaspekte – Performance-Analyse
- Nutzen und Mehrwert
  - Echtzeit-Status
  - Zentrale Darstellung aller Informationen
  - Einfach zu verstehen
  - Einfach zu verwalten

ISA 2004 Monitoring Tools

- **Übersicht** – Aggregierte, zentralisierte Ansicht
- **Alarme** – Ein Platz für alle Probleme
- **Sitzungen** – Ansicht der aktiven Sitzungen
- **Dienste** – Status der ISA Dienste
- **Berichte** – Top User, Top Sites, Cache, usw.
- **Konnektivität** – Konnektivität zu kritischen Netzwerkdiensten überprüfen
- **Protokollierung** – Aussagekräftige Darstellung der ISA Protokolle

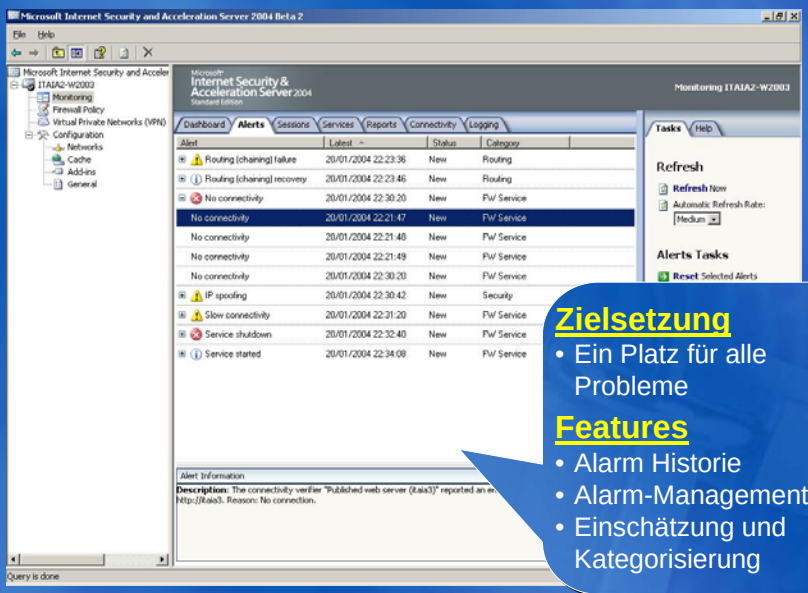
Übersicht



Zielsetzung
- Zentralisierte Statusansicht

Features
- Echtzeit
- Aggregierte Ansicht
- Schnelle Erkennung von Problemen

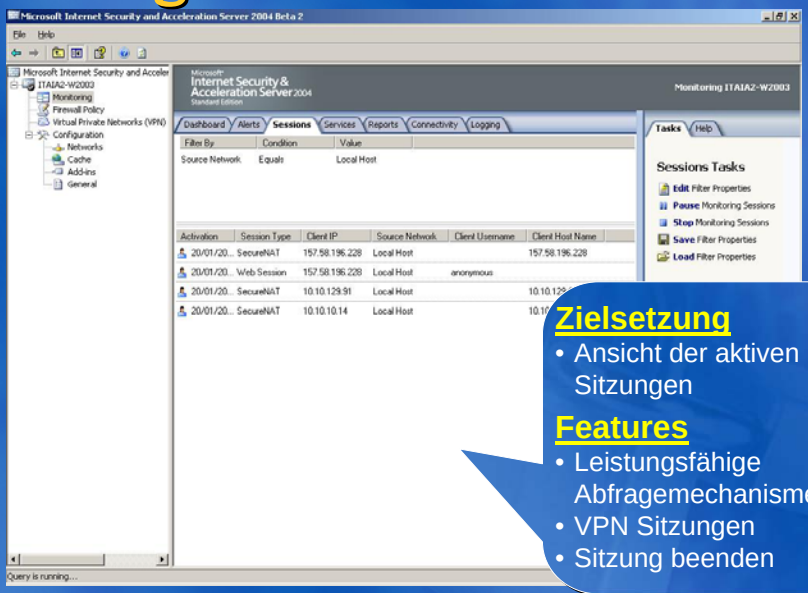
Alarme



Zielsetzung
- Ein Platz für alle Probleme

Features
- Alarm Historie
- Alarm-Management
- Einschätzung und Kategorisierung

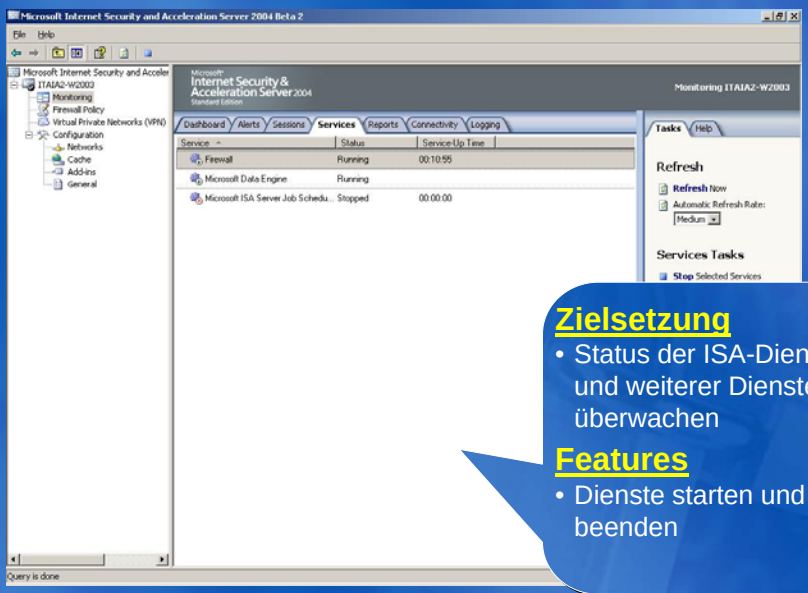
Sitzungen



Zielsetzung
- Ansicht der aktiven Sitzungen

Features
- Leistungsfähige Abfragemechanismen
- VPN Sitzungen
- Sitzung beenden

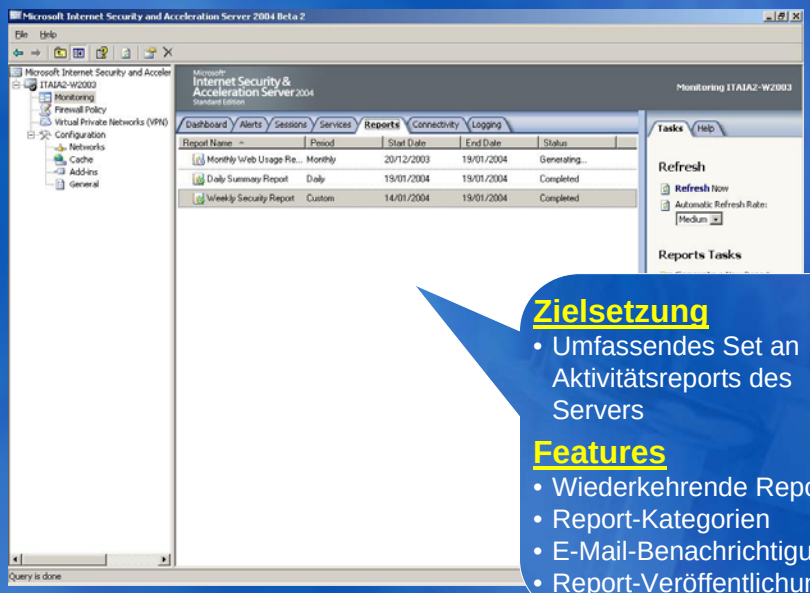
Dienste



Zielsetzung
- Status der ISA-Dienste und weiterer Dienste überwachen

Features
- Dienste starten und beenden

Berichte



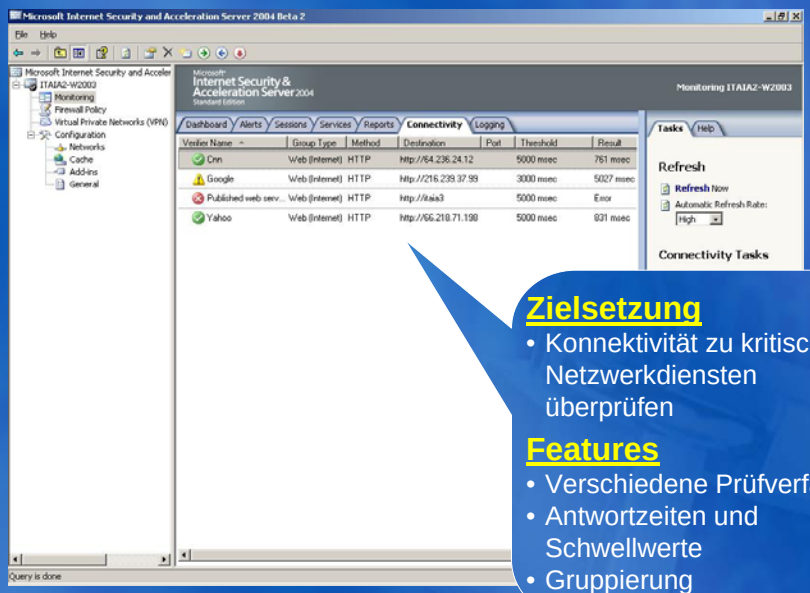
Zielsetzung

- Umfassendes Set an Aktivitätsreports des Servers

Features

- Wiederkehrende Reports
- Report-Kategorien
- E-Mail-Benachrichtigung
- Report-Veröffentlichung

Konnektivität



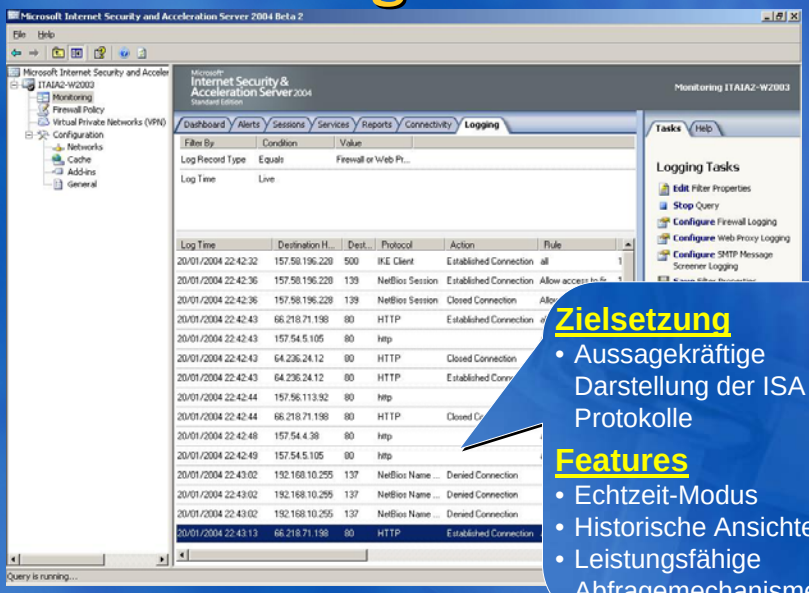
Zielsetzung

- Konnektivität zu kritischen Netzwerkdiensten überprüfen

Features

- Verschiedene Prüfverfahren
- Antwortzeiten und Schwellwerte
- Gruppierung

Protokollierung



Zielsetzung

- Aussagekräftige Darstellung der ISA Protokolle

Features

- Echtzeit-Modus
- Historische Ansichten
- Leistungsfähige Abfragemechanismen

ISA Server 2004 New Features

Weitergeführtes Engagement für Integration

Hohe Performance

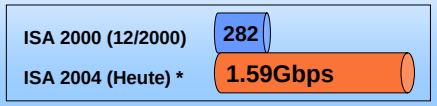
Nachgewiesene Eignung für Filterung auf Applikations-Ebene

Optimierte Architektur	• High speed Datentransport • Nutzt aktuellste Hardware • SSL bridging entlastet Downstream-Server
Web Cache	• Upgedatete Richtlinien • Inhalt wird lokal bereitgestellt • Pre-fetching während niedriger Aktivität
Internet-Zugangskontrolle	• Benutzer- und Gruppenbasierte Regeln • Erweiterbar durch Drittanbieter

Performance

- Architektur für hohe Performance optimiert
  - Optimiert für reale Einsatzszenarien
  - *"Raw throughput"* wurde mithilfe von HTTP- und NAT-Benchmarks ermittelt
  - Kernelmodus Datenpumpe; Benutzermodus Optimierungen
  - Skalierbar durch den Einsatz zusätzlicher CPUs

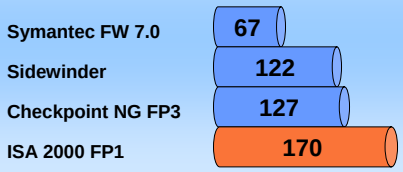
Raw throughput Performance [Mbps]:



* Ergebnisse der Beta-Version

Wie?
- Design Verbesserungen
- IP Stack Verbesserungen
- Hardware Verbesserungen

Network computing magazine
app. level firewalls review (3/03)
full inspection performance [Mbps]:



Zusammenfassung

- ISA Server Beta ist bereits zum Download verfügbar unter:
  http://www.microsoft.com/isaserver/beta/default.asp
- Wichtige Verbesserungen:
  - Hochentwickelte Schutzmechanismen
  - Einfache Nutzbarkeit (Ease of use)
  - Hohe Performance
- Hilft dem Kunden, sich vor der wachsenden Anzahl von Sicherheitsproblemen auf Applikationsebene zu schützen


Microsoft®
© 2003 Microsoft Corporation. All rights reserved.
This presentation is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.