Internetanbindung für ein Unternehmen realisieren

Inhaltsverzeichnis

1 Proxy-Server / ISA-Server Aufgaben 4
1.1 Vorbereitung 4
1.2 Aufgaben / Lösungen 4
1.2.1 Aufgabe 1 4
1.2.2 Aufgabe 2 4
1.2.3 Aufgabe 3 5
1.2.4 Aufgabe 4 5
1.2.5 Aufgabe 5 5
1.2.6 Aufgabe 6 6
1.2.7 Aufgabe 7 6
1.2.8 Aufgabe 8 7
1.2.9 Aufgabe 9 7
1.2.10 Aufgabe 10 10
1.2.11 Aufgabe 11 10
1.2.12 Aufgabe 12 11
1.2.13 Aufgabe 13 11
1.2.14 Aufgabe 14 11
1.2.15 Aufgabe 15 11
1.2.16 Aufgabe 16 11
1.2.17 Aufgabe 17 11
1.2.18 Aufgabe 18 11
1.2.19 Aufgabe 19 12
1.2.20 Aufgabe 20 12
1.2.21 Aufgabe 21 12
1.2.22 Aufgabe 22 12
1.2.23 Aufgabe 23 12
1.2.24 Aufgabe 24 13
1.2.25 Aufgabe 25 13
1.2.26 Aufgabe 26 13
1.2.27 Aufgabe 27 13
1.2.28 Aufgabe 28 13
1.2.29 Aufgabe 29 13
1.2.30 Aufgabe 30 13
1.2.31 Aufgabe 31 14
1.2.32 Aufgabe 32 14
1.2.33 Aufgabe 33 14
1.2.34 Aufgabe 34 14
1.2.35 Aufgabe 35 14
1.2.36 Aufgabe 36 14
1.2.37 Aufgabe 37 15
1.2.38 Aufgabe 38 15
1.2.39 Aufgabe 39 15
1.2.40 Aufgabe 40 15
1.2.41 Aufgabe 41 15
2 Videokonferenz mit FW und WLAN 16
2.1 Vorbereitung 16
2.2 Aufgaben / Lösungen 16
2.2.1 Aufgabe 1 16
2.2.2 Aufgabe 2 16
2.2.3 Aufgabe 3 19

2.2.4 Aufgabe 4 ... 19
2.2.5 Aufgabe 5 ... 20
2.2.6 Aufgabe 6 ... 21
2.2.7 Aufgabe 7 ... 23
2.2.8 Aufgabe 8 ... 23
2.2.9 Aufgabe 9 ... 24
2.2.10 Aufgabe 10 ... 26
3 CheckPoint Firewall mit 2 NW Interfaces ... 28
3.1 Vorbereitung ... 28
3.2 Aufgaben / Lösungen ... 28
3.2.1 Aufgabe 1 ... 28
3.2.2 Aufgabe 2 ... 30
3.2.3 Aufgabe 3 ... 30
3.2.4 Aufgabe 4 ... 30
3.2.5 Aufgabe 5 ... 30
3.2.6 Aufgabe 6 ... 30
3.2.7 Aufgabe 7 ... 30
3.2.8 Aufgabe 8 ... 30
3.2.9 Aufgabe 9 ... 30
4 Routing ... 30
4.1 Vorbereitung ... 30
4.2 Aufgaben / Lösungen ... 30
4.2.1 Aufgabe 1 ... 30
4.2.2 Aufgabe 2 ... 30
4.2.3 Aufgabe 3 ... 30
4.2.4 Aufgabe 4 ... 30
4.2.5 Aufgabe 5 ... 30
4.2.6 Aufgabe 6 ... 30
4.2.7 Aufgabe 7 ... 30
4.2.8 Aufgabe 8 ... 30
4.2.9 Aufgabe 9 ... 30
4.2.10 Aufgabe 9 ... 30

1 Proxy-Server / ISA-Server Aufgaben

1.1 Vorbereitung

Folgende Geräte werden eingerichtet:

- 1 PC mit Windows 2003 Server, zwei Netzwerkkarten und Microsoft ISA Server.
- 2 PCs mit Windows 2000/XP, je eine Netzwerkkarte.
- 2 Hub/Switches
- 4 Patchkabel, RJ45

1.2 Aufgaben / Lösungen

1.2.1 Aufgabe 1

ISA Server ist in zwei Versionen verfügbar, Standard Edition und Enterprise Edition. Die Versionen verfügen über denselben umfangreichen Featuresatz, wobei die Standard Edition nur auf einem einzelnen Server mit maximal vier Prozessoren läuft. Für komplexere Installationen, Serverarrayunterstützung, Sicherheitsrichtlinien für mehrere Ebenen und Computer mit mehr als vier Prozessoren benötigen Sie ISA Server Enterprise Edition.

Quelle: http://www.msisafaq.de/Anleitungen/2000/Grundlagen/was_ist_isa.htm

1.2.2 Aufgabe 2

Der ISA Server verfügt u.A. über folgende Standard Features:

- Sicheres Veröffentlichen
- Active Caching
- Weit reichende Anwendungsunterstützung
- Programmierbare Cachesteuerung
- Verteiltes und hierarchisches Caching
- SSL-Verkehr-Inspektion
- Integriertes VPN (Virtual Private Networking)
- Leistungsstarker Webcache
- Erweiterte Authentifizierung
- Systemsicherung
- Download nach Plan
- Intuitive Benutzeroberfläche
- Integrierte Berichterstellung
- Bandbreitenprioritäten
- Remoteverwaltung
- Intelligente Anwendungsfilter
- Vereinheitlichte Verwaltung
- Mehrstufiger Firewall
- Skalierbarkeit
- Windows 2000 Integration
- E-Mail-Inhaltsüberprüfung
- Transparenz für alle Clients
- Integriertes Erkennen unberechtigter Zugriffe

- Stateful Inspection
- Medienstreamingunterstützung
- Mehrstufige Zugriffsrichtlinien
- Detailliertes Protokollieren
- Überwachen und Warnen
- Verwaltung mehrerer Server

Quelle: http://www.msisafaq.de/Anleitungen/2000/Grundlagen/was_ist_isa.htm

1.2.3 Aufgabe 3

Clientadresssätze sind ein wichtiger Bestandteil der Richtlinienkonfiguration eines ISA-Servers. Sie ermöglichen es, einzelne oder mehrere Computer (basierend auf ihren IP-Adressen) in Gruppen zusammenzufassen. Die Clientadresssätze können für Serververöffentlichungsregeln und Protokollregeln verwendet werden. Sie sind hilfreich, um Zugriffe auf Ziele einzuschränken. Clientadresssätze können sowohl interne als auch externe IP-Adressen beinhalten, jedoch keine Computer- oder Benutzernamen.

Clientadresssätze werden z.B. verwendet um eine Serververöffentlichung nur bestimmten externen Zielen zugänglich zu machen. Beispielsweise kann damit der Zugriff auf einen internen SQL-Server nur einem Kunden, dessen Gateway-IP-Adresse bekannt ist, zugänglich gemacht werden. Oder der SQL-Server kann nur von einem Server in der DMZ erreicht werden.

Andersherum ist es auch möglich, festzulegen, dass nur bestimmte IP-Adressen des internen Netzwerkes (z.B. nur die Server) das SMTP-Protokoll ausgehend nutzen können.

Quelle: http://www.msisafaq.de/Anleitungen/2000/Grundlagen/ClientAdressSet.htm

1.2.4 Aufgabe 4

Betriebssystem	Ja	Nein	Bemerkung
Windows 98		x	
Windows 98 SE		x	
Windows ME		x	
Windows NT 3x/4.0		x	
Windows 2000		x	
Windows 2000 Server	x		Service Pack 1
Windows 2000 Advanced Server	x		Service Pack 1
Windows 2000 Datacenter Server	x		Service Pack 1
Windows 2003 Standard Server	x		
Windows 2003 Web Server	x		
Windows 2003 Enterprise Server	x		
Windows 2003 Datacenter Server	x		

1.2.5 Aufgabe 5

Der ISA kann in drei Betriebsmodi installiert werden:

- ***Caching-Modus***
  Im Cachemodus kann die Netzwerkleistung gesteigert und Bandbreite

eingespart werden, indem häufig zugegriffene Objekte im Speicher des ISA Server zwischengelagert werden. Es können interne Webserver für den Zugriffe aus dem Internet veröffentlicht werden.

- ***Firewall-Modus***
  Im Firewall-Modus kann anhand von Regeln die Kommunikation zwischen dem Firmennetzwerk und dem Internet gesteuert und abgesichert. Ausserdem können interne Server veröffentlicht werden.

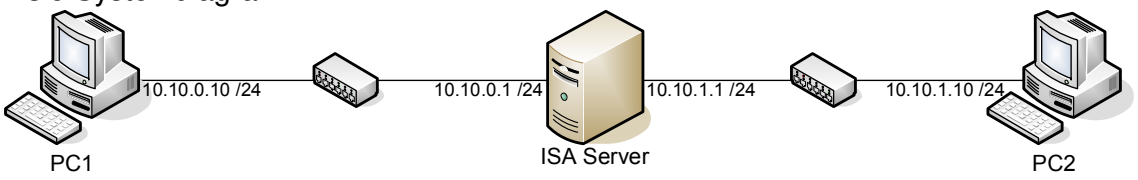
- ***Integrierter Modus***
  Im Integrierten Modus stehen alle Funktionen zur Verfügung.

Die folgende Tabelle gibt eine Übersicht über die in den jeweiligen Modi enthaltenen/möglichen Funktionen:

Funktion	Firewallmodus	Cachemodus
Protokolldefinitionen /-regeln	Ja	nur HTTP, HTTPS, FTP, Gopher
Paketfilter	Ja	Nein
Cache Konfiguration	Nein	Ja
Unternehmensrichtlinien (nur Enterprise Edition)	Ja	Ja
Unterstützung für Firewall- und SecureNAT-Client	Ja	Nein
Unterstützung für Webproxyclient	Ja	Ja
Echtzeit-Überwachung	Ja	Ja
Berichte	Ja	Ja
Mindestanzahl Netzwerkschnittstellen erforderlich	2	1
Web Filter	Ja	Ja
Webveröffentlichungen	Ja	Ja
Serververöffentlichung	Ja	Nein
Virtuelle Private Netzwerke (VPN)	Ja	Nein
Bandbreitenrichtlinien	Ja	Nein
Anwendungsfilter	Ja	Nein
LAT/LDT	Ja	Nein

1.2.6 Aufgabe 6

Visio Systemdiagramm:

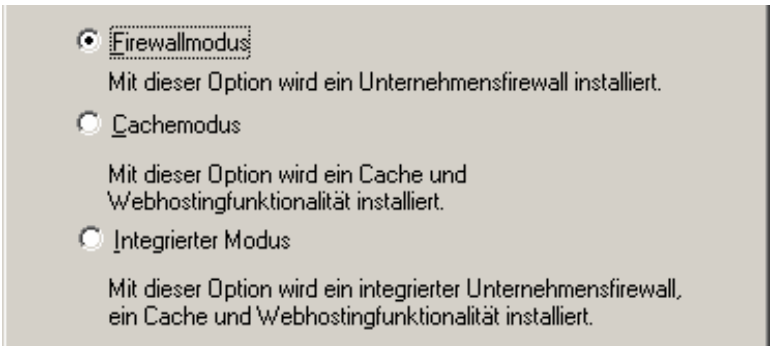


1.2.7 Aufgabe 7

- ISA Server CD einlegen und Setup starten.
- „ISA Server installieren“ wählen.
- Hinweis, dass nach der Installation SP1 für ISA Server 2000 installiert werden muss, wird mit „weiter“ bestätigt.

- Benutzerdefinierte Installation wählen.

- Gültige Seriennummer eingeben.
- Anschliessend wird darauf aufmerksam gemacht, dass dieser Server an keiner Domäne angemeldet ist.
- Im nächsten Schritt kann einer von drei möglichen Installationsmodi gewählt werden. Wir entscheiden uns den ISA Server als Firewall zu installieren.



- Bereits während der Installation werden vom Assistenten die beiden Netzwerkadressbereiche verlangt. Unsere beiden Netze verlaufen
  → von 10.10.0.0 bis 10.10.0.255 (Netz 1)
  und
  → von 10.10.1.0 bis 10.10.1.255 (Netz 2)
- Gleich nach dem der Assistent die Installation beendet hatte, installierten wir Service Pack 1 und 2 für ISA Server 2000.

1.2.8 Aufgabe 8

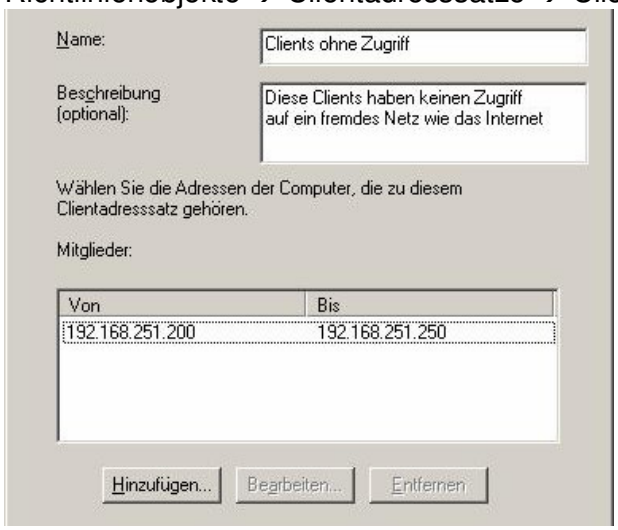
In Aufgabe 7 wird verlangt, dass der ISA Server als Firewall aufgesetzt wird.
Während der Installation kann die Option „Firewallmodus“ gewählt werden.
Der Cache-Modus beitet nicht in erster Linie sicherheitsrelevante Funktionen, sondern steigert lediglich die Leistung, indem Internetseiten in einen Cache gelegt werden.
(Siehe Aufgabe 5 für die Unterschiede der verschiedenen Modi).

1.2.9 Aufgabe 9

Computer mit den Adressen 192.168.251.200 - 192.168.251.200 dürfen nicht ans Netz.

- ISA Server Verwaltung starten.

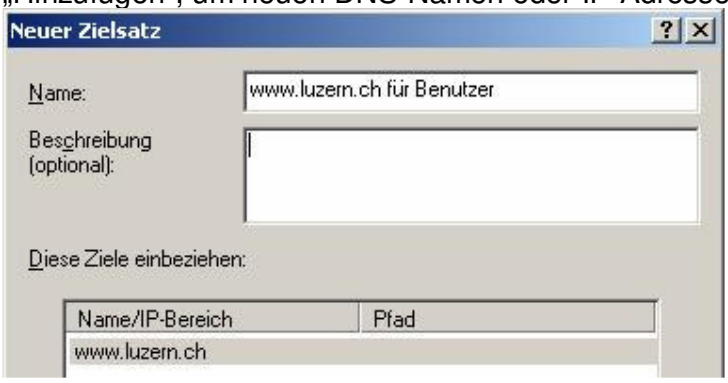
- Richtlinienobjekte → Clientadresssätze → Clientadresssatz hinzufügen.



- Zugriffsrichtlinie → Site- und Inhaltsregeln → Site- und Inhaltsregel hinzufügen.
- Assistent startet. Hier werden diverse Angaben gemacht:
  → Name: Kein Zugriff.
  → Antwort auf Zugriffsanfrage des Clients: Verweigern.
  → Regel anwenden für: alle Ziele.
  → Zeitplan verwenden: Immer.
  → Regel anwenden für Anfragen von: Speziellen Computers (Clientadresssätzen).

Mitglieder der Gruppe Benutzer dürfen die Site www.luzern.ch erst ab 14:00 Uhr aufsuchen.

- Richtlinien → Zielsätze → Zielsatz erstellen.
- „Hinzufügen“, um neuen DNS-Namen oder IP-Adresse hinzuzufügen.



- Richtlinien → Zeitplan → Zeitplan erstellen.

- Zugriffsrichtlinie → Site- und Inhaltsregeln → Site- und Inhaltsregel erstellen.
- Assistent startet. Hier werden diverse Angaben gemacht:
  → Name: Zugriff Benutzergruppe
  → Antwort auf Zugriffsanfrage des Clients: Zulassen.
  → Regel anwenden für:

  → Zeitplan verwenden: Zeitplan für www.luzern.ch
  → Regel anwenden für Anfragen von: Spezielle Benutzer und Gruppen.
- Gruppe „ISA\Benutzer“ hinzufügen.

Der Zugriff auf die Seiten: www.beateuhse.de, www.praline.de, soll nicht erlaubt sein.

- Richtlinien → Zielsätze → Zielsatz erstellen.
- Name: SexSites
- Mit „Hinzufügen“ die beiden auszuschliessenden DNS-Namen eintragen:
  → www.beateuhse.de
  → www.praline.de
- Zugriffsrichtlinie → Site- und Inhaltsregeln → Site- und Inhaltsregel erstellen.
- Assistent startet. Hier werden diverse Angaben gemacht:
  → Name: SexSites blockieren.
  → Antwort auf Zugriffsanfrage des Clients: Verweigern.
  → Regel anwenden für: SexSites
  → Zeitplan verwenden: Immer
  → Regel anwenden für Anfragen von: Jeder Anfrage.

Einkäufer dürfen nur auf die Seiten www.arp.ch, www.kmelektronik.de zugreifen.

- Neue (lokale) Benutzergruppe „Einkäufer“ erstellen.
- Richtlinien → Zielsätze → Zielsatz erstellen.

- Name: Einkaufsseiten
- Mit „Hinzufügen“ die beiden zugelassenen DNS-Namen eintragen:
  → www.arp.ch
  → www.kmelektronik.ch
- Zugriffsrichtlinie → Site- und Inhaltsregeln → Site- und Inhaltsregel erstellen.
- In der ersten Siteregel für die Einkäufer werden ALLE Anfragen blockiert:
  → Name: Einkäufer (verweigern)
  → Antwort auf Zugriffsanfrage des Clients: Verweigern.
  → Regel wird anwenden für: Alle Ziele.
  → Zeitplan verwenden: Immer.
  → Regel anwenden für Anfragen von: Jeder Anfrage.
- In der zweiten Siteregel für die Einkäufer werden vordefinierte Anfragen zugelassen:
  → Name: Einkäufer (zulassen)
  → Antwort auf Zugriffsanfrage des Clients: Zulassen.
  → Regel anwenden für: Einkaufsseiten.
  → Zeitplan verwenden: Immer.
  → Regel anwenden für Anfragen von: Spezielle Benutzer und Gruppen.
- Gruppe „ISA\Einkäufer“ hinzufügen.

1.2.10 Aufgabe 10

Tests mit diversen weiteren Regeln durchgeführt.

1.2.11 Aufgabe 11

Statische URL Filter werden in den Aufgaben 9 und 10 dokumentiert. Dynamische URL Filter filtern alle Websites, welche einen bestimmten Inhalt haben.
Der ISA Server bietet jedoch von Haus aus keinen sog. Contentfilter. Um diese Funktionalität zu implementieren, kann ein Dienst wie „Burstek Webfilter“ installiert werden.
Mit diesem Filter können Website nach bestimmten Kategorien gefiltert werden.

1.2.12 Aufgabe 12

Der ISA Server 2000 verfügt standardmässig über einen eigenen Leistungsmonitor. In diesem ISA Server-Leistungsmonitor können diverse Parameter gemessen werden:

- Belegter Cache
- Workerthreads
- Anfragen pro Zeitraum
- u.v.m.

1.2.13 Aufgabe 13

Die Proxyeinstellungen auf den Arbeitsstationen werden nicht verändert. Ein Proxyserver muss den Clients nicht angegeben werden, da der installierte ISA Server als Firewall und nicht als Proxyserver fungiert.

Um den ISA Server lauffähig zu machen wurden folgende Schritte durchgeführt:

- Default Gateways definieren:
  → GW für PC1: 10.10.0.1
  → GW für PC2: 10.10.1.1
- Internet Informationsdienst auf PC2 installieren.
- Auf dem Computer „ISA“ in der Routingkonsole „Routing und RAS aktivieren“.

Ziel Netzwerk	Subnetzmaske	Gateway	Schnittstelle
10.10.0.0	255.255.255.0	10.10.0.1	10.10.0.1
10.10.1.0	255.255.255.0	10.10.1.1	10.10.1.1

- Hosts Dateien werden bei beiden Clients sowie beim Server mit den entsprechenden Namen und IP-Adressen ergänzt. Beispiel Hosts Datei von PC1:

```
10.10.0.1          isa
10.10.1.10         pc2
```

1.2.14 Aufgabe 14

Siehe Aufgabe 13.

1.2.15 Aufgabe 15

-

1.2.16 Aufgabe 16

-

1.2.17 Aufgabe 17

-

1.2.18 Aufgabe 18

-

1.2.19 Aufgabe 19

Content-Screening zeichnet jeglichen Netzwerkverkehr auf. Wenn eine Session die Policy verletzt, wird die Session abgebrochen und/oder der Administrator informiert. Der Administrator kann im Log nachvollziehen, welcher Benutzer zu welcher Zeit welche Informationen abgerufen hat und welche Policy dabei verletzt wurde.

1.2.20 Aufgabe 20

Der ISA-Server liefert von Haus aus sehr viele Protokolldefinitionen mit (siehe Protokolldefinitionen.xls), die jedoch jederzeit erweitert werden können und meist auch müssen. Eine Liste der standardmässigen Protokolldefinitionen kann hier gefunden werden.

Protokolldefinitionen sind die Grundlage für sämtliche Zulassungs-/Verweigerungsregeln und Veröffentlichungsregeln. Sie müssen stets vor der Konfiguration der jeweiligen Regel erstellt werden. Diese Definitionen sind quasi Vorlagen. Die mitgelieferten Protokolldefinitionen können nicht verändert oder gelöscht werden.

Protokolldefinitionen.xls

1.2.21 Aufgabe 21

Protokollregeln legen fest, mit welchen Protokollen interne Clients Zugriff auf das Internet haben. Protokollregeln können eine oder mehrere Protokolldefinitionen beinhalten, deren Zugriff sie erlauben oder verweigern.
Für die häufigsten Protokolle sind bereits fertige Protokolldefinitionen vorhanden, eigene können jederzeit hinzugefügt werden.

1.2.22 Aufgabe 22

Fragt ein Client ein Objekt mit einem bestimmten Protokoll an, überprüft ISA Server die Protokollregeln. Wenn eine Protokollregel ausdrücklich die Verwendung des Protokolls verweigert, wird die Anfrage verweigert. Die Anfrage wird weiterhin nur dann verarbeitet, wenn eine Protokollregel es dem Client ausdrücklich erlaubt, mit dem betreffenden Protokoll zu kommunizieren und wenn eine Site- und Inhaltsregel ausdrücklich den Zugriff auf das angefragte Objekt zulässt.

Protokollregeln gelten für Firewallclients und sichere Netzwerkadressübersetzungsclients (SecureNAT-Clients). Ist das Protokoll durch ein Anwendungsfilter definiert, gilt die Protokollregel für Firewall- und SecureNAT-Clients. Gilt die Protokollregel für ein Protokoll, das nur eine primäre Verbindung besitzt (z. B. HTTP), gilt die Regel für Firewall- und SecureNAT-Clients.

1.2.23 Aufgabe 23

Wenn man bei SecureNAT-Clients eine Protokollregel definiert, die für den gesamten IP-Datenverkehr gelten soll, wird die Regel tatsächlich nur auf alle definierten Protokolle angewendet.

1.2.24 Aufgabe 24

→ Firewallmodus
→ Cachemodus
→ Integrierter Modus

1.2.25 Aufgabe 25

Ein Wechsel des Modus im laufenden Betrieb ist nicht möglich, hierzu muss eine Neuinstallation ("drüber installieren") erfolgen. Die bisherige Konfiguration bleibt prinzipiell erhalten; allerdings nur die Objekte, die im neuen Modus verfügbar sind. Wenn also z.B. vom Integrierten Modus zum Cachemodus gewechselt wird, gehen alle Protokolldefinitionen, Serververöffentlichungen, IP-Paketfilter verloren.

1.2.26 Aufgabe 26

Die Paketfilterungsfunktion des ISA Servers ermöglicht die Steuerung des Flusses von IP-Paketen von und zum ISA Server. Wenn die Paketfilterung aktiviert wird, werden alle Pakete auf der externen Schnittstelle verworfen, wenn sie nicht ausdrücklich zugelassen werden. Die Zulassung kann entweder statisch, durch IP-Paketfilter, oder dynamisch, durch Zugriffsrichtlinien oder Veröffentlichungsregeln erfolgen. Auch wenn keine Paketfilterung aktiviert ist, wird die Kommunikation zwischen dem lokalen Netzwerk und dem Internet nur zugelassen, wenn ausdrücklich Regeln konfiguriert wurden, die den Zugriff zulassen.

In den meisten Fällen ist es vorzuziehen, Ports dynamisch zu öffnen. Daher erfolgt die Empfehlung, Zugriffsrichtlinienregeln, die internen Clients den Zugriff zum Internet erlauben, bzw. Veröffentlichungsregeln, die externen Clients den Zugriff auf interne Server gestatten, zu erstellen. Dies liegt daran, weil IP-Paketfilter die Ports statisch öffnen. Zugriffsrichtlinien und Veröffentlichungsregeln öffnen die Ports jedoch dynamisch (sobald eine Anfrage ankommt).

1.2.27 Aufgabe 27

Vordefinierte Zeitpläne können in Protokollregeln, Bandbreitenregeln sowie in Site- und Inhaltsregeln verwendet werden. Dadurch kann zum Beispiel konfiguriert werden, dass bestimmte Mitarbeiter nur in der Mittagspause auf bestimmte Webseiten (z.B. Sportnachrichten) zugreifen dürfen.

1.2.28 Aufgabe 28

Wenn der ISA Server im Firewallmodus oder im integrierten Modus installiert wird, muss während des Installationsvorgangs die lokale Adresstabelle (LAT) angegeben werden. Die lokale Adresstabelle ist eine Tabelle aller internen IP-Adressbereiche, die im internen Netzwerk hinter dem ISA Server-Computer verwendet werden. Der ISA Server steuert anhand der LAT, wie Computer im internen Netzwerk mit externen Netzwerken kommunizieren.

1.2.29 Aufgabe 29

Im Gegensatz zur LAT enthält die LDT keine IP-Adressbereiche sondern Domänennamen.

1.2.30 Aufgabe 30

Der ISA Server unterscheidet drei Arten von Clients:

- SecureNAT-Client

- Webproxyclient
- Firewallclient

1.2.31 Aufgabe 31

Der SecureNAT Client ist der am einfachsten zu konfigurierende Client. Es muss lediglich sichergestellt werden, dass das Default-Gateway des Rechners auf den ISA-Server zeigt. In grossen Umgebungen mit zwischengeschalteten Routern muss lediglich der letzte Router in der Kette den ISA als Standard-Gateway eingetragen haben. SecureNAT-Client ist betriebssystemunabhängig; jedes TCP/IP-basierende System kann ein SecureNAT Client werden.

1.2.32 Aufgabe 32

Damit ein Client ein Webproxyclient wird, muss im Browser der ISA-Server als Proxy eingetragen werden. Dies ist ebenfalls unabhängig vom Betriebssystem; der Browser muss jedoch HTTP 1.1-CERN kompatibel sein, was jedoch die meisten gängigen Browser sind.

1.2.33 Aufgabe 33

Der letzte Client-Typ erfordert die Installation der Firewallclient-Software des ISA-Servers und wird nur auf folgenden Betriebssystemplattformen unterstützt: Windows 95 OSR2, Windows 98/ME, Windows NT 4.0, Windows 2000/XP/2003.

1.2.34 Aufgabe 34

Inhaltsgruppen fassen bestimmte Datentypen zusammen (z.B. Texte, Audiodateien, Viedeodateien) ISA- Server besitzt eine Reihe vordefinierter Inhaltsgruppen. Der Dateityp wird nur in der Windowswelt durch die Dateierweiterungen bestimmt. Andere Betriebssysteme verwenden MIME- Typen (Multipurpose Internet Mail Extension). MIME Type steht in der Datei (am Anfang) und kann vom Benutzer nicht geändert werden.

1.2.35 Aufgabe 35

Eine Volumenbeschränkung gibt es im ISA Server nicht. Zu meiner Enttäuschung auch keine Limitierungsmöglichkeit der Übertragungsgeschwindigkeit. Unter ISA können jedoch Bandbreitenprioritäten vergeben werden. Mit dieser Funktion können Benutzer, Gruppen oder Services untereinander priorisiert werden.
Folgende beiden Software Tools ermöglichen eine Geschwindigkeitsbegrenzung:
→ Websense
→ NetPeeker

1.2.36 Aufgabe 36

Das Backup der ISA Server-Konfiguration sollte eine Selbstverständlichkeit sein, zumal der ISA eine wesentliche und wichtige Komponente einer Netzwerkinfrastruktur darstellt. Aus diesem Grund enthält die ISA Verwaltungskonsole eine Sicherungs- und Wiederherstellungsfunktion. Damit können die Konfigurationsdaten von eigenständigen Servern und Arrays in einer Datei (lokal oder auf einem Netzwerklaufwerk) gespeichert werden.
Die Sicherungs-/Wiederherstellungsfunktion kann nicht dazu verwendet werden, die Konfiguration eines ISA Servers auf einen anderen zu übertragen (klonen).

1.2.37 Aufgabe 37

Alle allgemeinen Konfigurationsinformationen werden gesichert. Dazu gehören:

- Zugriffsrichtlinienregeln
- Veröffentlichungsregeln
- Richtlinienelemente
- Alarmkonfiguration
- Cachekonfiguration
- ISA Server-Eigenschaften

1.2.38 Aufgabe 38

Einige serverspezifische Konfigurationsinformationen werden nicht gesichert. Dazu gehören:

- Cacheinhalt
- Aktivitätsprotokolle
- Berichte

Hinweis

Mit dem Windows-Sicherungsprogramm können ISA Server-Informationen, wie z. B.

- Kennwörter
- lokale Registrierungsparameter
- Konfigurationsinformationen des Cachespeichers
- H.323-Gatekeeperkonfiguration
- Berichte
- lokale Einstellungen für Anwendungsfilter
- Parameter für die Leistungsoptimierung
- Cacheinhalte und Protokolldateien

gesichert werden.

1.2.39 Aufgabe 39

Für die Wiederherstellung nach einem Systemausfall wird die Sicherung der gesamten Computerkonfiguration benötigt. Deshalb sollte ein regelmässiges Backup der Systemdaten erfolgen. Das ISA-eigene Backup kann nicht automatisiert werden. Die ISA Konfiguration sollte jedes Mal vor- und nach Änderungen der Einstellungen durchgeführt werden.

1.2.40 Aufgabe 40

Über den Remoteadministrationsclient kann der komplette ISA Server administriert werden. Mit folgenden Ausnahmen:

- Die Berichte können nicht eingesehen werden
- Der VPN-Einrichtungs-Wizzard steht nicht zur Verfügung
- Die Backup-Restore-Funktion steht nicht zur Verfügung

1.2.41 Aufgabe 41

Der ISA Server kann via Microsoft Terminal Server Client administriert werden. Diese Remotedesktop Software kann via „Start“ → „Ausführen“ → „mstsc /console“ gestartet werden.

2 Videokonferenz mit FW und WLAN

2.1 Vorbereitung

Folgende Geräte werden eingerichtet:

- 2 PCs mit Windows 2000/XP mit WLAN Netzwerkadapter
- 2 WLAN Kameras
- 1 ZyWALL 10W mit WLAN Netzwerkadapter
- div. Patchkabel / serielle Verbindungskabel

2.2 Aufgaben / Lösungen

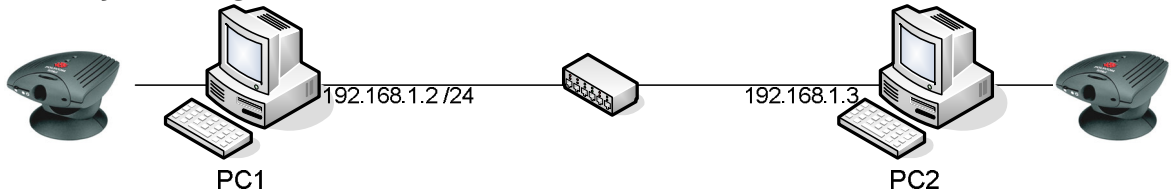
2.2.1 Aufgabe 1

- Kameras an beiden Computer einstecken. Wichtig: Nicht einschalten, vor die Software installiert ist!
- Polycom ViaVideo Software von der Herstellerwebsite herunterladen.
- Software installieren und anschliessend starten.
- Beim ersten Start von ViaVideo wird ein Assistent gestartet, welcher einige Konfigurationsdaten entgegen nimmt.
- Sprachwahl: German.
- Benutzername und E-Mail Adresse werden gefordert. Diese Angaben müssen im Falle einer Registrierung bei Polycom korrekt eingetragen werden.

- Verzeichnisserver werden keine eingetragen. Letztere markierte werden deaktiviert.
- Im nächsten Setupschritt wird ein Admin-Kennwort eingetragen. Dieses Kennwort wird für den Zugang zur Webschnittstelle der Software benötigt.
- In den nächsten Schritten wird das Audio-Setup vorgenommen. Lautsprecher- und Mikrophon werden justiert.
- Netzwerk-Setup: Lokale IP-Adresse verweden.

2.2.2 Aufgabe 2

Visio Systemdiagramm:



Videokonferenz herstellen:

- Kameras an beiden Computern einschalten.
- Polycom ViaVideo starten.

- Anrufschaltfläche betätigen.

- Neue Kontakte werden mit der Schaltfläche „Neu“ hinzugefügt.
  Beispiel des Konferenzpartners:

- Der neue Kontakt wird in der Übersicht angezeigt. Per Doppelklick oder beim Drücken der „Anruf“-Schaltfläche wird eine Verbindung zum Konferenzpartner hergestellt.

- Der Konferenzpartner wird informiert. Er kann die Verbindung annehmen bzw. ablehnen. Nimmt das Gegenüber die Verbindung an, so wird nach einem kurzen Moment das lokale Bild durch das Bild der Remote-Kamera ersetzt.
- Mit der Schaltfläche „PIP“ (was soviel wie „Picture In Picture“ bedeutet) kann zusätzlich zum Bild der Remote-Kamera auch das Bild der lokalen Kamera

angezeigt werden:

Whiteboard-Funktion

Mit ViaVideo kann man während eines Videoanrufs zusammen mit anderen Konferenzteilnehmern auf einem für alle freigegebenen Whiteboard zeichnen.

- Auf „Anrufsteuerungen“ → „Daten-Sharing" klicken, um die NetMeeting-Bedienelemente aufzurufen.
- Auf „Ein“ klicken, um die Funktionen zu aktivieren.
- Auf „Whiteboard starten“klicken, um die Whiteboard-Anwendung zu starten.

Weitere Informationen über den Gebrauch des NetMeeting-Whiteboards sind in der Online Hilfe erhältlich.

Textbasierte Chat-Funktion

Mithilfe der Chat-Funktion kann man Textnachrichten an Teilnehmer senden.

- Auf „Anrufsteuerungen“ → „Daten-Sharing" klicken, um die NetMeeting-Bedienelemente aufzurufen.
- Auf „Ein“ klicken, um die Funktionen zu aktivieren.
- Auf „Chat starten“ klicken.
- Im Dialogfeld „Nachricht“ die gewünschte Nachricht eingeben und deren Empfänger auswählen.
- Auf „Nachricht senden“ klicken, um die Nachricht zu senden.

Dateien übertragen und empfangen

Die Dateiübertragung ist häufig der letzte Schritt nach dem Anzeigen oder Zusammenarbeiten, damit die Teilnehmer das aktuellste Exemplar des Dokuments erhalten, an dem sie während der Sitzung gearbeitet haben.
Wenn an dem Anruf mehrere teilnehmen, wird die Datei an alle Mitwirkende geschickt.

<u>Datei senden:</u>

- Auf „Anrufsteuerungen“ → „Daten-Sharing" klicken, um die NetMeeting-Bedienelemente aufzurufen.
- Auf „Ein“ klicken, um die Funktionen zu aktivieren.

- Auf „Datei übertragen“ klicken, um das Dialogfeld „Dateiübertragung“ zu öffnen.
- Auf "Dateien hinzufügen" klicken, um die Dateien auszuwählen, die übertragen werden sollen.
- Personen auswählen, die die Datei erhalten sollen, oder „Alle“ wählen, um sie an alle Teilnehmer des Anrufs zu senden.

Datei empfangen:

- Wenn das Dialogfeld „Dateien empfangen“ eingeblendet wird, auf „Annehmen“ klicken.
- Die empfangenen Dateien werden unter der Verzeichnisadresse „C:\Programmdateien\NetMeeting\Empfangene Dateien“ kopiert.

2.2.3 Aufgabe 3

Grundlegende Einstellungen

ViaVideo erlaubt es, grundlegende Bildeinstellungen vorzunehmen. Die Kamera justiert die Helligkeit, Kontrast und Bildschärfe automatisch, doch diese Einstellungen sind nicht immer optimal. Es empfiehlt sich daher noch manuelle Nachkorrekturen vorzunehmen.

Kamerabedienelemente

- Auf „Anrufsteuerungen“ → „Kamerabedienelemente" klicken, um die Kameraeinstellungen aufzurufen.
- Bei Bedarf die Bildeinstellung korrigieren.

2.2.4 Aufgabe 4

→ Erfolgreich durchgeführt.
→ Keine Mikrophone vorhanden.

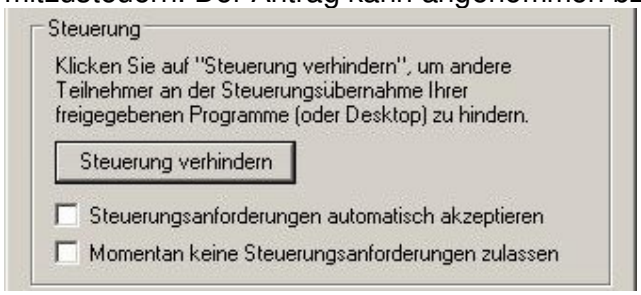
2.2.5 Aufgabe 5

- Application-Sharing muss in den Einstellungen von ViaVideo aktiviert werden. Dazu wird das Setup geöffnet.

- In der Registerkarte „Daten“ ist folgende Option zu aktivieren.

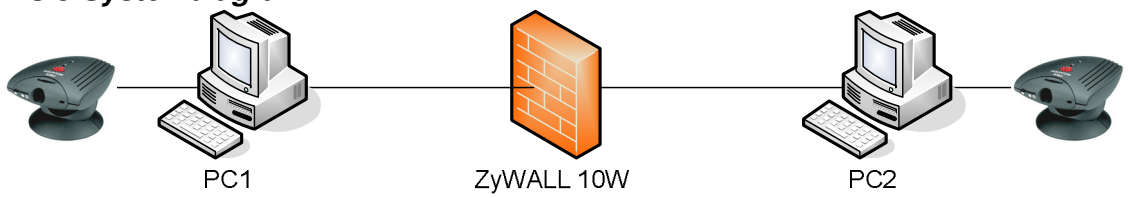
- Computer neu starten. Anschliessend ViaVideo wieder ausführen.
- Auf „Anrufsteuerungen“ → „Daten-Sharing" klicken.
- Auf „Ein“ klicken, um die Funktionen zu aktivieren.
- „Anwendung auswählen…“ wählen.
- Im Fenster sind alle aktiven Anwendungen aufgelistet. Hier kann individuell eine Anwendung ausgeführt und geteilt werden. Wird der „Desktop“-Eintrag gewählt, so kann der gesamte Bildschirm geteilt werden. Die Auswahl wird mit „Freigeben“ für den Konferenzpartner freigeben.

- Im selben Fenster kann mit einer Schaltfläche die Steuerung für den Konferenzpartner zugelassen bzw. verweigert werden. Ist die Steuerung zugelassen, so kann das Gegenüber einen Antrag stellen, um auch mitzusteuern. Der Antrag kann angenommen bzw. abgelehnt werden.



2.2.6 Aufgabe 6

Visio Systemdiagramm



	PC1	ZyWALL 10W	PC2
IP Adresse	192.168.1.2	192.168.1.1 (LAN) 192.168.2.1 (WAN)	192.168.2.2
Subnetzmaske	255.255.255.0	255.255.255.0	255.255.255.0
Default Gateway	192.168.1.1	-	192.168.2.1

ZyWALL Firewall konfigurieren

Bevor wir jegliche Konfigurationen anrühren, ändern wir gleich beim ersten Start das Admin-Kennwort. Ein grosses Sicherheitsloch entsteht, wenn das Initialpasswort des Herstellers (meistens „1234“) nicht geändert wird.
Die Zywall fordert den Administrator bereits beim ersten Start auf, das Kennwort zu ändern.
Die IP Konfiguration der Firewall wurde via Telnet vorgenommen, wobei wir für die Konfiguration der Firewall auf das Webinterface wechseln mussten.

<u>IP Konfiguration</u>

- Am LAN PC1 starten wir eine Telnetverbindung mit „telnet 192.168.1.1“ auf die Firewall. Der WAN Client PC2 hat keinen Zugriff!
- Menüpunkt „3. LAN Setup“ wählen.

```
                    ZyWALL 10W Main Menu

Getting Started                     Advanced Management
  1. General Setup                    21. Filter and Firewall Setup
  2. WAN Setup                        22. SNMP Configuration
  3. LAN Setup                        23. System Password
  4. Internet Access Setup            24. System Maintenance
                                      26. Schedule Setup
                                      27. VPN/IPSec Setup
Advanced Applications
  11. Remote Node Setup
  12. Static Routing Setup
  15. NAT Setup
```

- Menüpunkt „2. TCP/IP and DHCP Setup“ wählen.
- Folgende Einstellungen werden vorgenommen:
  → DHCP = None
  → IP Address = 192.168.1.1
  → IP Subnet Mask = 255.255.255.0

```
            Menu 3.2 - TCP/IP and DHCP Ethernet Setup

DHCP= None                          TCP/IP Setup:
Client IP Pool:
  Starting Address= N/A             IP Address= 192.168.1.1
  Size of Client IP Pool= N/A       IP Subnet Mask= 255.255.255.0
First DNS Server= N/A               RIP Direction= Both
  IP Address= N/A                     Version= RIP-1
Second DNS Server= N/A              Multicast= None
  IP Address= N/A                   Edit IP Alias= No
Third DNS Server= N/A
  IP Address= N/A
DHCP Server Address= N/A
```

- Zurück zum Hauptmenü navigieren und anschliessend zum Menüpunkt „4. Internet Access Setup“ navigieren.
- Hier werden folgende Einstellungen vorgenommen:
  → IP Address Assignment = Static
  → IP Address = 192.168.2.1
  → IP Subnet Mask = 255.255.255.0
  → Gateway IP Address = 0.0.0.0
  → NAT = None

Firewall Konfiguration

- Internet Explorer starten und auf „http://192.168.1.1“ zugreifen.
- Admin-Kennwort eingeben. (Passwort ändern, falls noch nicht geändert).
- Menüpunkt „System“ → Registerkarte „Time Settings“.
- Hier wird die korrekte Uhrzeit und Datum eingetragen, denn beim protokollieren schreibt die Firewall jeweils genaue Zeitangaben in den Log.
- Zum Menüpunkt „Firewall“ wechseln.

- Packet Direction: „*LAN to WAN*“
  → Pakete, die der/den Firewall-Regel(n) nicht entsprechen: „block“ (Standardeinstellung).
  → Alle Pakete, welcher der/den Firewall-Regel(n) nicht entsprechen, sollen geloggt werden.
  → Neue Regel hinzufügen, mit folgenden Eigenschaften:

Source Address	Destination Address	Service Type	Action
192.168.1.2 /24	192.168.2.2 /24	Video1 (TCP/UDP:3230-3235) Video2 (TCP:1720) Video3 (TCP:1731) Video4 (TCP:1503	Forward

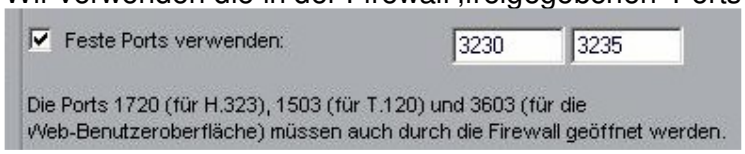
- Packet Direction: „*WAN to LAN*“
  → Pakete, die der/den Firewall-Regel(n) nicht entsprechen: „block“ (Standardeinstellung).
  → Alle Pakete, welcher der/den Firewall-Regel(n) nicht entsprechen, sollen geloggt werden.
  → Neue Regel hinzufügen, mit folgenden Eigenschaften:

Source Address	Destination Address	Service Type	Action
192.168.2.2 /24	192.168.1.2 /24	Video1 (TCP/UDP:3230-3235) Video2 (TCP:1720) Video3 (TCP:1731) Video4 (TCP:1503	Forward

ViaVideo konfigurieren

- ViaVideo Setup öffnen.

- In der Registerkarte „Netzwerk“ wird die Option „Feste Ports verwenden“ aktiviert.
- Wir verwenden die in der Firewall ‚freigegebenen’ Ports 3230 bis 3235:



Hinweis: Netzwerkadressübersetzung (NAT)

NAT-Netzwerkumgebungen verwenden interne IP-Adressen für die im Netzwerk befindlichen Geräte und eine externe IP-Adresse für die Kommunikation mit der „Aussenwelt“ (WAN). Eine NAT verwendet private Adressen.
Die meisten mit Kabelmodems und digitalen Teilnehmerleitungen (DSL) benutzten Router bieten diese Netzwerkadressübersetzung. Wenn Sie einen Router verwenden, muss Ihrem Videokonferenz-Endpunkt eine öffentliche IP-Adresse zugeordnet sein, damit eine Kommunikation mit der Außenwelt möglich ist.

Vor der Konfiguration der ViaVideo-Anwendungen für den Gebrauch hinter einer NAT müssen Sie die folgenden festen Ports öffnen:

- Port 389 (TCP): Für ILS-Registrierung
- Port 1503 (TCP): Microsoft NetMeeting T.120-Daten-Sharing
- Port 1718 (UDP): Gatekeeper-Erkennung
- Port 1719 (UDP): Gatekeeper-RAS (muss bidirektional sein)
- Port 1720 (TCP) H.323-Anrufs-Setup (muss bidirektional sein)
- Port 1731 (TCP): Steuerung von Audio-Anrufen (muss bidirektional sein)
- Ports 3230-3235 (TCP/UDP): Signale und Steuerung von Audio, Anrufen, Video und Daten/FECC
- Port 3603 (TCP): ViaVideo Web-Schnittstelle

2.2.7 Aufgabe 7

→ Keine andere Anmeldung am Router (z.B. via Telnet oder Seriell) darf aktiv sein.
→ „LAN to LAN/ZyWALL“ bzw. „WAN to WAN/ZyWALL“ (je nach Bedürfnis) muss aktiviert werden, d.h. der entsprechende Radiobutton wird auf „Forward“ gestellt.

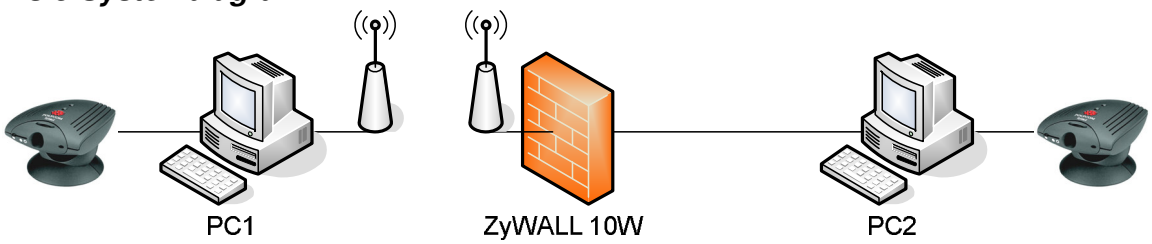
2.2.8 Aufgabe 8

- Damit wir sicher sind, dass keinen Verkehr von LAN zu WAN und umgekehrt gelangt, senden wir ein einfacher PING von PC1 (192.168.1.2) zu PC2 (192.168.2.2).

- Im Log der Firewall sehen wir kurz danach einen Eintrag mit dem blockierten ICMP Packet.

2.2.9 Aufgabe 9

Visio Systemdiagramm



	PC1	ZyWALL 10W	PC2
IP Adresse	192.168.1.3	192.168.1.1 (LAN) 192.168.2.1 (WAN)	192.168.2.2
Subnetzmaske	255.255.255.0	255.255.255.0	255.255.255.0
Default Gateway	192.168.1.1	-	192.168.2.1

WLAN installieren

Als Erweiterung zur Aufgabe 6 ff. wird in der PC1 in Aufgabe 9 mit WLAN erschlossen. Der Client wird folglich mit einem WLAN Adapter (USB) ausgestattet, während die ZyWALL 10W bereits über einen PCMCIA Slot verfügt und lediglich durch einen WLAN Adapter (PCMCIA) erweitert werden muss.

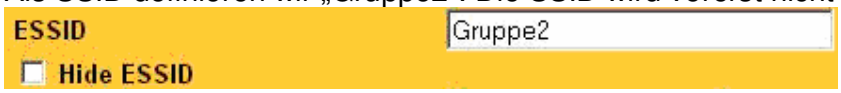
<u>WLAN Adapter installieren</u>

- Software von Herstellerwebsite herunterladen.
- Setup starten. (Wichtig: USB WLAN Adapter darf nicht eingesteckt werden, bevor das Setup beendet wurde!)
- Nachdem das Setup beendet wurde, wird der USB WLAN Adapter angeschlossen.
- Unter „Systemsteuerung“ → „Netzwerkverbindungen“ → „Drahtlose Netzwerkverbindung“ wird in den Eigenschaften die IP-Adresse „192.168.1.3“ mit der Subnetzmaske „255.255.255.0“ eingetragen. (Gateway: „192.168.1.1“).

<u>Firewall Konfiguration</u>

- Via Internet Explorer auf „http://192.168.1.1“ zugreifen und einloggen.
- Unter Menüpunkt „Wireless LAN“ wird die Checkbox „Enable Wireless LAN“ aktiviert.

- Als SSID definieren wir „Gruppe2“. Die SSID wird vorerst nicht versteckt.



- Zum Menüpunkt „Firewall“ wechseln.
- Packet Direction: „*<u>LAN to WAN</u>*“
  → Pakete, die der/den Firewall-Regel(n) nicht entsprechen: „block“ (Standardeinstellung).
  → Alle Pakete, welcher der/den Firewall-Regel(n) nicht entsprechen, sollen geloggt werden.

→ Bestehende Regel anpassen. Die Quelladresse ist nun nicht mehr die LAN Verbindung (192.168.1.2) sondern die WLAN Verbindung (192.168.1.3):

Source Address	Destination Address	Service Type	Action
192.168.1.**3** /24	192.168.2.2 /24	Video1 (TCP/UDP:3230-3235) Video2 (TCP:1720) Video3 (TCP:1731) Video4 (TCP:1503	Forward

- Packet Direction: „*WAN to LAN*“
  → Pakete, die der/den Firewall-Regel(n) nicht entsprechen: „block“ (Standardeinstellung).
  → Alle Pakete, welcher der/den Firewall-Regel(n) nicht entsprechen, sollen geloggt werden.
  → Bestehende Regel anpassen. Die Zieladresse ist nun nicht mehr die LAN Verbindung (192.168.1.2) sondern die WLAN Verbindung (192.168.1.3):

Source Address	Destination Address	Service Type	Action
192.168.2.2 /24	192.168.1.**3** /24	Video1 (TCP/UDP:3230-3235) Video2 (TCP:1720) Video3 (TCP:1731) Video4 (TCP:1503	Forward

ViaVideo konfigurieren

- ViaVideo Setup öffnen.

- In der Registerkarte „Netzwerk“ wird die lokale IP-Adresse (von ursprünglich „192.168.1.2“) auf „192.168.1.3“ gewechselt.

Videokonferenz testen

- WLAN Client erkennt die SSID „Gruppe2“ und verbindet sich automatisch. Bei USB WLAN Adapter kann es öfters zu Problemen kommen. Meistens hilft hier ein Neustart des Computers.
- In der ViaVideo Software von PC2 wird nun im Adressbuch noch die neue IP-Adresse von PC1 eingetragen.
  → Die Netzwerkgeschwindigkeit ist bemerkbar langsamer geworden.
  → Im WLAN wurden derzeit noch keine sicherheitsrelevanten Einstellungen vorgenommen!

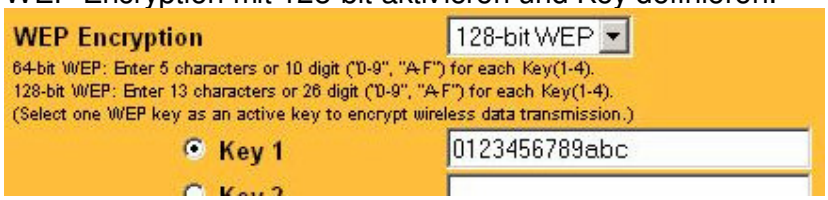
WLAN Sicherheit erhöhen

SSID verstecken

- Auf dem WLAN Client PC1 wird zuerst die SSID „Gruppe2“ in der Konfigurationssoftware von Zyxel manuell eingetragen.
- Via Webschnittstelle loggen wir uns auf der Firewall ein.
- Unter Menüpunkt „Wireless LAN“ wird die Checkbox „Hide ESSID“ aktiviert. Mit dieser Einstellung wir die SSID nicht mehr gebroadcasted. Dies bringt zwar nicht in erster Linie „Übertragungssicherheit“, sondern verhindert das Aufspüren des WLAN’s durch triviale Sniffer Software.

WEP Verschlüsselung

- WEP Encryption mit 128-bit aktivieren und Key definieren.



- Anschliessend Einstellungen auf Firewall speichern und Browser verlassen.
- In der Konfigurationssoftware von Zyxel navigieren wird zur Registerkarte „Konfiguration“. Hier finden wir die Schaltfläche „Sicherheit“. Im nachfolgenden Fenster werden die Einstellungen vervollständigt:

MAC Filter

Damit nur noch der PC1 mit dem WLAN Access Point kommunizieren kann wird auf der ZyWALL ein MAC Filter eingerichtet.

- Unter Menüpunkt „Wireless LAN“, Registerkarte „MAC Filter“ wird die Checkbox „Active“ aktiviert.
- In die Tabelle wird die MAC Adresse von PC1 eingetragen:

- Einstellungen auf Firewall speichern und Browser schliessen.

2.2.10 Aufgabe 10

Radius Server Authentication

RADIUS („Remote Authentication Dial-In User Service“) ist ein Client-Server-Protokoll, das zur Authentifizierung von Benutzern bei Einwahlverbindungen in ein Computernetzwerk dient. RADIUS ist der Standard bei der zentralen Authentifizierung von Einwahlverbindungen über Modem, ISDN, VPN oder Wireless LAN.
Ein spezieller Server-Dienst, der RADIUS-Server, dient dabei der Authentifizierung von Clientgeräten oder Diensten gegen unterschiedliche Datenbanken, in denen die Zugangsdaten (zum Beispiel Benutzername und Passwort) gespeichert sind.

MAC Filter

MAC Filtering ist ein eifacher Mechanismus mit einer relativ hohen Sicherheit. Die MAC-Adressen von den Clients werden in Access Control Lists (ACL) auf dem Access-Point gespeichert. Diese Sicherheitsimplementierung ist wegen des grossen Verwaltungsaufwands nur in privaten Netzwerken praktizierbar.

WEP Encryption
Wired Equivalent Privacy (WEP) ist der Standardverschlüsselungsalgorithmus für WLAN. Er soll sowohl den Zugang zum Netz regeln, als auch die Integrität der Daten sicherstellen.

Wi-Fi Protected Access
WPA ist eine Verschlüsselungsmethode für ein Wireless LAN. Nachdem sich die Wired Equivalent Privacy (WEP) des IEEE-Standards 802.11 als unsicher erwiesen hatte und sich die Verabschiedung des neuen Sicherheitsstandards 802.11i verzögerte, wurde durch die Wi-Fi eine Teilmenge von 802.11i vorweggenommen und unter dem Begriff WPA als Pseudostandard etabliert.
WPA bietet zusätzlichen Schutz durch dynamische Schlüssel, die auf dem Temporal Key Integrity Protocol (TKIP) basieren, und bietet optional die Anmeldung von Nutzern über das Extensible Authentication Protocol (EAP) an.
Die erhöhte Sicherheit gegenüber WEP besteht darin, dass der Schlüssel nur bei der Initialisierung verwendet wird und anschließend ein Session-Key zum Einsatz kommt.

DES
Der Data Encryption Standard (kurz: DES) ist ein weit verbreiteter symmetrischer Verschlüsselungsalgorithmus. Seine Entstehungsgeschichte hat immer wieder großen Anlass zu Spekulationen gegeben und sei hier kurz wiedergegeben.
Nachteil: Weil die Schlüssellänge nur 56-bit beträgt, konnte DES bereits durch Brute Force - Angriffe gebrochen werden, indem systematisch alle Schlüssel getestet wurden.

AES
Der Advanced Encryption Standard (AES) ist ein symmetrisches Kryptosystem, welches als Nachfolger für DES bzw. 3DES im Oktober 2000 vom National Institute of Standards and Technology (NIST) als Standard bekannt gegeben wurde. Nach seinen Entwicklern Joan Daemen und Vincent Rijmen wird er auch Rijndael-Algorithmus genannt.

3 CheckPoint Firewall mit 2 NW Interfaces

3.1 Vorbereitung

Folgende Geräte werden eingerichtet:

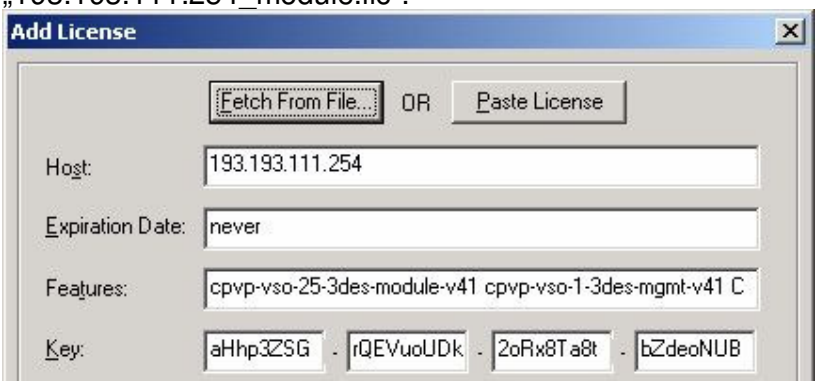
- 1 PC mit Windows 2000 Server, zwei Netzwerkkarten.
- 2 PCs mit Windows 2000/XP, je eine Netzwerkkarte.
- 2 Hub/Switches
- 4 Patchkabel, RJ45

3.2 Aufgaben / Lösungen

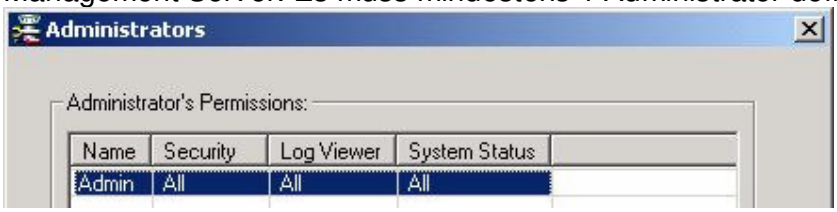
3.2.1 Aufgabe 1

Firewall installieren

- Checkpoint FW-1 Software entpacken und Setup starten.
- Installationstyp: „Stand Alone“
- VPN-1/FireWall-1 Gateway Module mit Limitation auf 25-250 Hosts.
- Installation ohne Rückwärtskompatibilität.
- Installationsordner definieren.
- Der Installationsassistent verlangt eine Lizenzdatei. Wir wählen die Datei „193.193.111.254_module.lic“.



- Im nächsten Schritt wird mit der Schaltfläche „Add…“ ein neues Administratorkonto eröffnet. Berechtigte Administratoren erhalten Zugriff zum Management Server. Es muss mindestens 1 Administrator definiert werden.



- Wird im nächsten Schritt „Control IP Forwarding“ gewählt, so werden KEINE IP Pakete weitergeleitet, wenn keine Security Policy geladen ist. Wir entscheiden uns für diese Variante. Die Option „Do no control IP Forwarding“ ist ein grosses Sicherheitsrisiko, wenn keine Security Policy geladen ist! Sicherheitsrisiko!
- IP-Adresse definieren. (Die vorgegebene Adresse muss nicht dringend korrekt sein!!)
  → 192.168.1.1 (interne Schnittstelle).

- Mittels der Schaltfläche „Add“ werden neue GUI Clients hinzugefügt.
  → 192.168.1.1 (d.h. nur von der Firewall aus kann administriert werden. In grösseren Unternehmen könnten zugunsten besserer Administrierung weitere befugte Clients eingetragen werden).
- Interface Name: Wird noch nicht festgelegt, da die Firewall zuerst mit den nötigen Patches versehen werden muss. Der Interface Name (des externen Interfaces) wird später eingetragen.
- Im nächsten Schritt verlangt der Assistent die willkürliche Eingabe von alphanumerischen Charakteren.

- Der Computer wird neu gestartet, sobald das Setup beendet ist.

Service Packs für Checkpoint FW-1 installieren

Folgende Service Packs werden installiert:

- ***Service Pack 4***
  → fw-1_41719_1_win2k_des.tgz
  → fwgui_41862_1_sp4_win32.tgz
- ***Service Pack 5***
  → fw-1_41_sp5_win32_vpn_des_new.tgz
  → fwgui_41_sp5_win32.tgz
- ***Service Pack 6***
  → fw-1-sp6-winnt-win2k-des-build41618-2-md5-9e3a3aa69ad77d78f1943276e6545843.tgz
  →fwgui-sp6-winnt-win2k-build41608-3-md5-e80a96b295ac0d7a8de1f80ea5b78de6.tgz

Hinweis
Die Installationsreihenfolge muss dringend eingehalten werden!

Routing aktivieren

- Routing und RAS Dienst unter „Systemsteuerung“ → „Software“ → „Windows Komponenten“ hinzufügen.
- Mit Rechtsklick auf den Server „FIREWALL“ → „Routing und RAS konfigurieren und aktivieren“ klicken. Assistent startet.

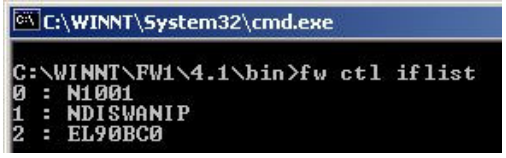
- Router soll ein einfacher Netzwerkrouter zwischen zwei TCP/IP Netzwerken sein.

- Im nächsten Schritt werden die installierten Protokolle angezeigt. Die Vorgabe wird mit „weiter“ bestätigt.

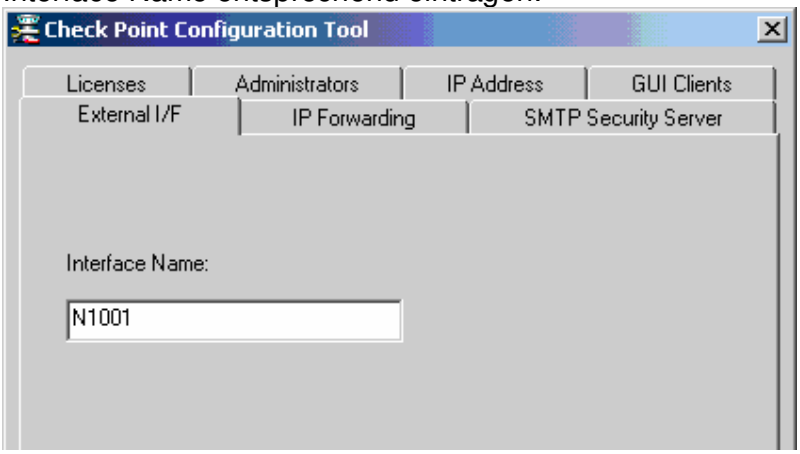
3.2.2 Aufgabe 2

Die Interface-Namen der von Checkpoint eingerichteten Schnittsstellen können über eine diensteigene Software ausfindig gemacht werden:

- Hierzu öffnen wir die Konsole („cmd“) und navigieren ins Verzeichnis
  `C:\WINNT\FW1\4.1\bin`
- Hier können mit dem Befehl
  `fw ctl iflist`
  die vorhanden Interfaces angezeigt werden.

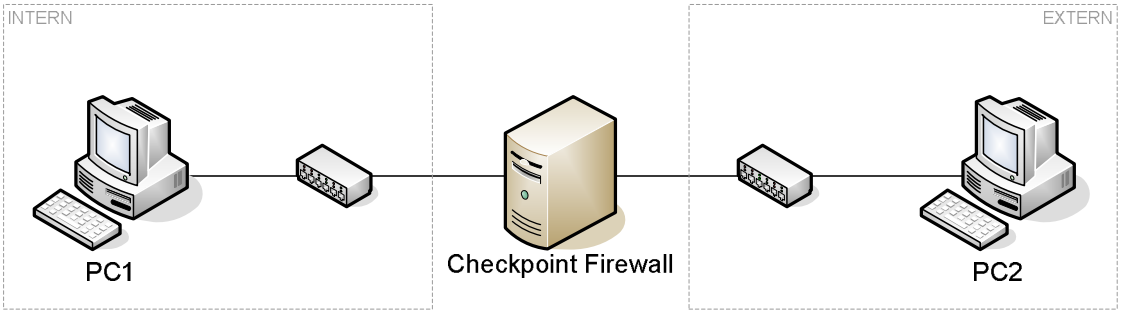


- Check Point Konfiguration starten („C:\WINNT\FW1\4.1\bin\cpconfig.exe“) → Registerkarte „External I/F“.
- Interface Name entsprechend eintragen:



3.2.3 Aufgabe 3

Visio Systemdiagramm



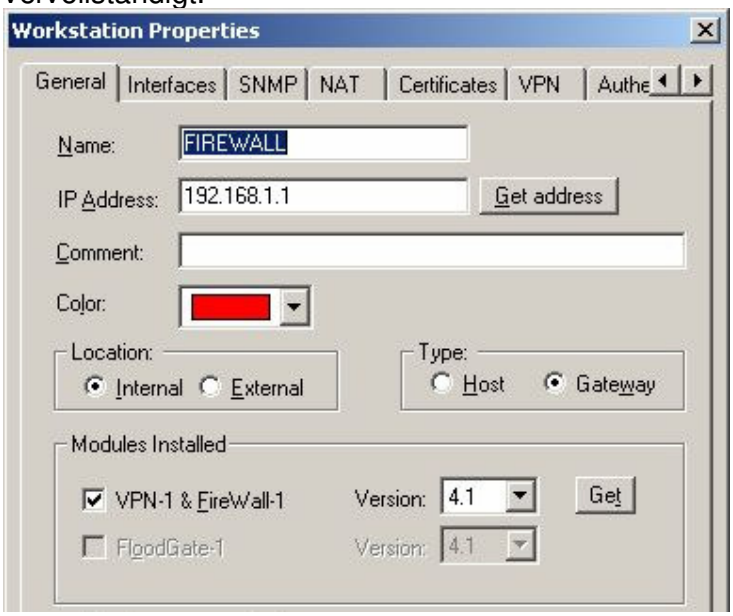
	PC1	Checkpoint FW-1	PC2
IP Adresse	192.168.1.2	INTERN : 192.168.1.1 EXTERN: 193.193.111.254	193.193.111.253
Subnetzmaske	255.255.255.0	INTERN : 255.255.255.0 EXTERN: 255.255.255.0	255.255.255.0
Default Gateway	192.168.1.1	INTERN : 193.193.111.254 EXTERN: 192.168.1.1	193.193.111.254

3.2.4 Aufgabe 4

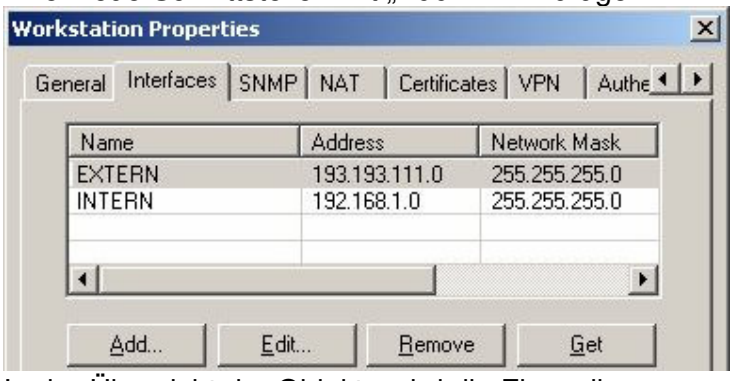
- CheckPoint Policy Editor starten („Start“ → „Programme“ → „Checkpoint Management Clients“).
- Mit berechtigtem Administrator-Account anmelden. (Angaben wurden während der Installation der Checkpoint Firewall definiert).

- Menü → „Edit“ → „Add Role“ → „Bottom“.
- Menü → „Edit“ → „Add Role“ → „Bottom“ (Die unterste Regel wird nicht verändert!! Sie soll alle nicht definierte Protokolle/Packetrichtungen sperren!)
- „Manage“ → „Network Obejcts“ → „New“ → „Workstation…“.

- In der Registerkarte „General“ werden die Angaben für die FIREWALL vervollständigt:



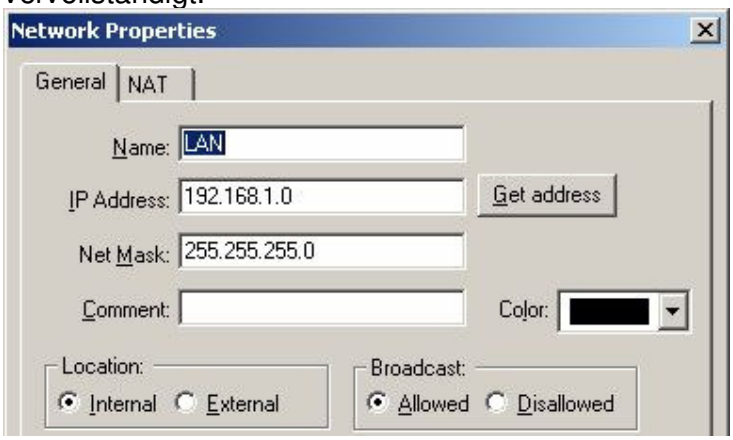
- Navigieren zur Registerkarte „Interfaces“.
- Zwei neue Schnittstellen mit „Add…“ hinzufügen.



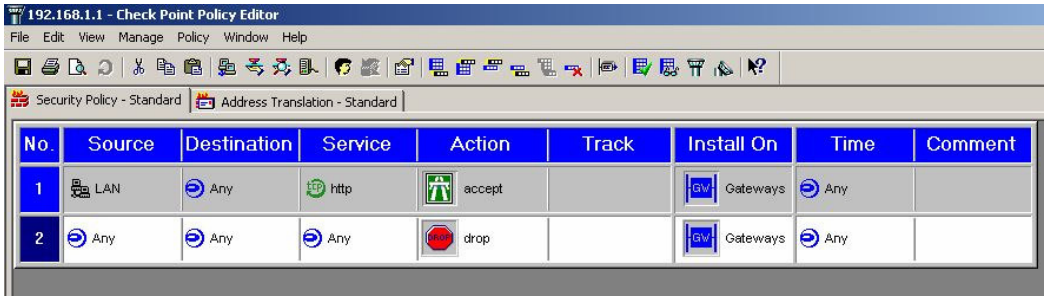
- In der Übersicht der Objekte wird die Firewall nun angezeigt:

- „Manage“ → „Network Obejcts“ → „New“ → „Network…“.

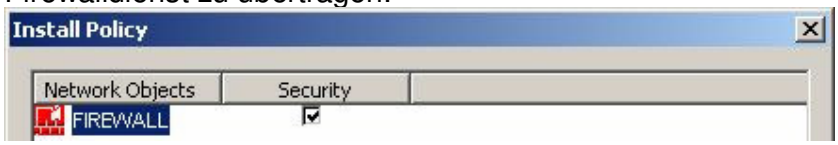
- In der Registerkarte „General“ werden die Angaben für die FIREWALL vervollständigt:



- Für die Regel Nr.1 wird nun definiert, dass die Quellgeräte aus dem „LAN“ alle Zielgeräte über das Protokoll „http“ ansprechen können.
  In der Regel Nr.2 wird, wie bereits erwähnt, der gesamte nicht in Regeln definiert Netzwerkverkehr blockiert.



- Menü „Policy“ → „Install“ wählen, um die Konfiguration vom GUI auf den Firewalldienst zu übertragen.

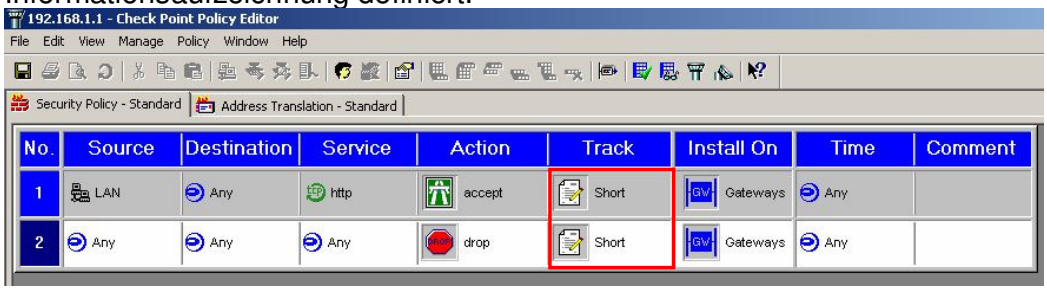


- Im Log die Aktualisierung mitverfolgt werden…

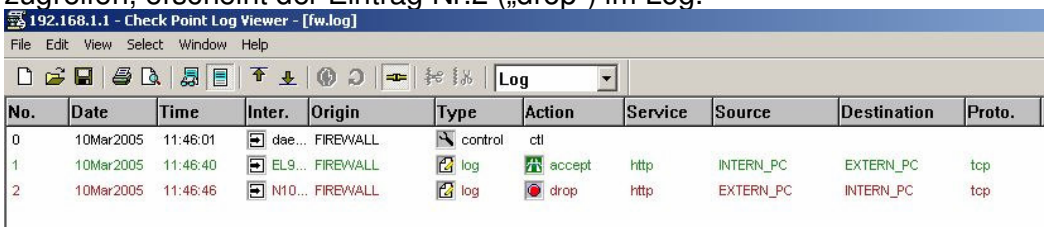
3.2.5 Aufgabe 5

- Damit die Firewall getestet werden kann, installieren wir auf dem internen Client (genannt: „INTERN_PC“) sowie auf dem externen Client (genannt: „EXTERN_PC“) den Internet Informationsdienst IIS6 und bereiten eine Testseite vor.

- Im Policy Editor wird in der Spalte „Track“ mit Rechtsklick die Art der Informationsaufzeichnung definiert.



- CheckPoint Policy Editor starten („Start“ → „Programme“ → „Checkpoint Management Clients“).
- Wenn wir vom Client „INTERN_PC“ auf „EXTERN_PC“’s Testwebsite zugreifen, erscheint der Eintrag Nr.1 („accept“) im Log.
  Wenn wir vom Client „EXTERN_PC“ auf „INTERN_PC“’s Testwebsite zugreifen, erscheint der Eintrag Nr.2 („drop“) im Log.

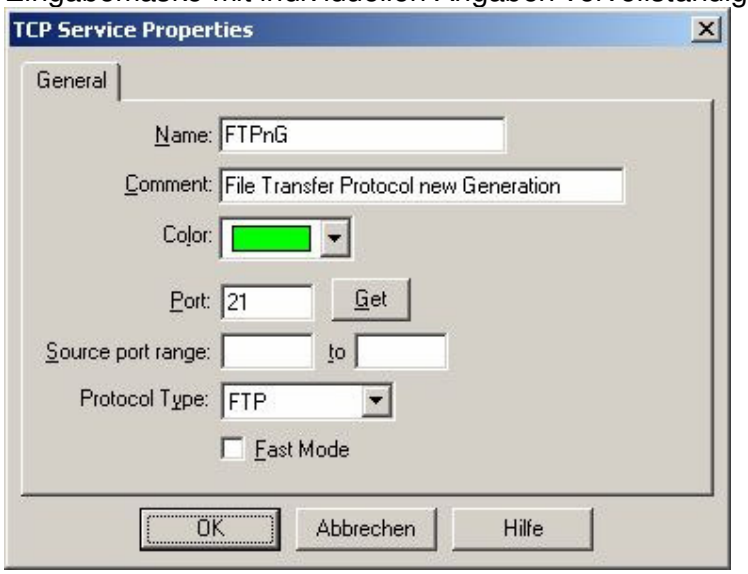


3.2.6 Aufgabe 6

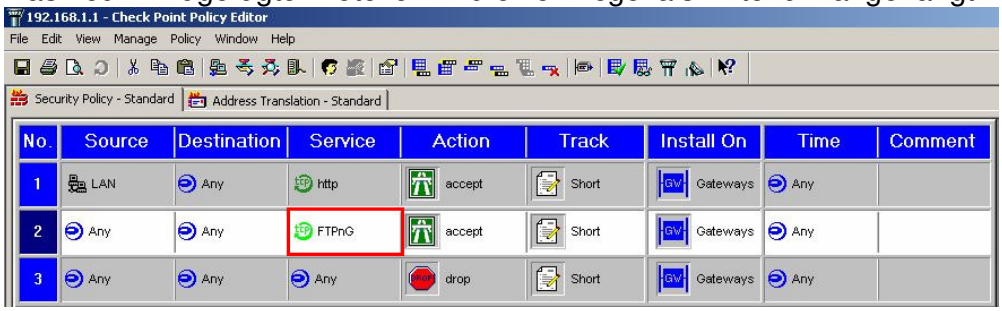
Siehe Aufgabe 1, Abschnitt „Routing aktivieren“.

3.2.7 Aufgabe 7

- Menü „Manage“ → „Services…“. Schaltfläche „New“.
- Eingabemaske mit individuellen Angaben vervollständigen:



- Das neu hinzugefügte Protokoll wird einer Regel als Kriterium angehängt.



3.2.8 Aufgabe 8

3.2.9 Aufgabe 9

Stateful Inspection ist ein Standard für Firewalls. Das Prinzip basiert darauf, dass jedes Datenpaket einer bestimmten aktiven Session zugeordnet wird. Dadurch lassen sich sogar stateless protocols wie z.B. UDP (User Datagram Protocol) überwachen. Die einzelnen Datenpakete werden anhand bestimmter Merkmale (z.B. IP-Adresse und Portnummer) zu einem logischen Datenstrom (je nach Hersteller "Session", "Flow" oder "Slot" genannt) zusammengefasst. Wesentlich ist, dass sowohl Hin- als auch Rückrichtung zum logischen Datenstrom gezählt werden. Dadurch werden auch Antwortpakete vom Firewall durchgelassen. Nicht zugehörige Pakete, z.B. solche die nicht innerhalb einer vorgegebenen Zeit eintreffen, werden verworfen.
Besteht ein Firewall aus mehreren Hardeware-Einheiten, von denen eine aktiv und die anderen Standby sind (Firewall-Cluster), so sind aufwändige Maßnahmen erforderlich, um die Standby-Geräte permanent über den aktuellen Zustand aller logischen Datenströme zu informieren (Synchronisation). Bei Ausfall des aktiven Firewalls kann dadurch ein Standby-Gerät sofort und ohne Paketverlust übernehmen.
Die Firma Check Point Software Technologies Ltd. nimmt für sich in Anspruch, diese Technik erfunden und patentiert zu haben.

Quelle: http://de.wikipedia.org/wiki/Stateful_inspection

4 Routing

4.1 Vorbereitung

Folgende Geräte werden eingerichtet:

-

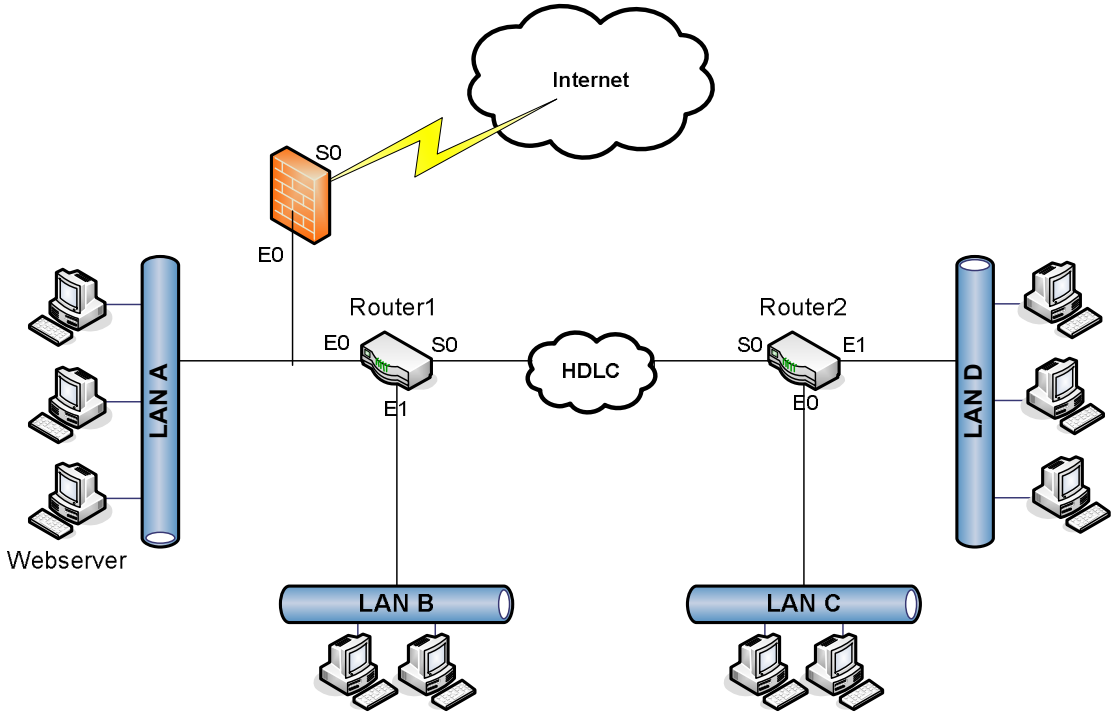
4.2 Aufgaben / Lösungen

4.2.1 Aufgabe 1

	LAN A	LAN B	LAN C	LAN D	TransitLAN
Netzwerk ID	10.0.0.0	10.0.7.0	10.0.4.0	10.0.6.0	10.0.7.64
Subnetzmaske	255.255.252.0	255.255.255.192	255.255.254.0	255.255.255.0	255.255.252.0
Broadcast	10.0.3.255	10.0.7.63	10.0.5.255	10.0.6.255	10.0.7.67
Gateway	10.0.3.254	10.0.7.62	10.0.5.254	10.0.6.254	10.0.7.66

4.2.2 Aufgabe 2

Visio Systemdiagramm



4.2.3 Aufgabe 3

Interface	Router1	Router2	Firewall/GW
Ethernet0	10.0.3.254	10.0.5.254	10.0.3.253
Ethernet1	10.0.7.62	10.0.6.254	
Serial0	10.0.7.66	10.0.7.65	DHCP (ISP)

4.2.4 Aufgabe 4

Die Netzgrössen werden so bestimmt, dass die IP-Adressen möglichst effizient genutzt werden können. Siehe Aufgabe 1.

4.2.5 Aufgabe 5

Konfiguration Router 1

Kommando	Bemerkung
router1>enable	Mit "enable" in den Admin-Modus wechseln.
router1#config terminal	Konfiguration via Terminal vornehmen.
router1(config)#ip subnet-zero	Beim Subnetting wird das erste Subnetz als Subnet-zero bezeichnet. Dieses wird hier zugelassen.
router1(config)#ip classless	Die Klassengrenzen (A,B,C…) warden mit dieser Option nicht mehr beachtet.
router1(config)#interface E0	Ethernet0 Schnittstelle auswählen.
router1(config-if)#ip address 10.0.5.254 255.255.254.0	IP-Adresse und Subnetzmaske für Ethernet0 definieren. Die weiteren Schnittstellen werden mit gleichem Vorgehen konfiguriert. Siehe Router-Config für Schnittstellen-Details.
router1(config-if)#no shut	Schnittstelle aktivieren.
router1(config)#exit	Config-Modus verlassen.
router1#write	Startup-Config wird mit Running-Config überschrieben.

E:\ÜK146\Routing\
Config Router1.txt

Konfiguration Router 2

Kommando	Bemerkung
router2>enable	Mit "enable" in den Admin-Modus wechseln.
router2#config terminal	Konfiguration via Terminal vornehmen.
router2(config)#ip subnet-zero	Beim Subnetting wird das erste Subnetz als Subnet-zero bezeichnet. Dieses wird hier zugelassen.
router2(config)#ip classless	Die Klassengrenzen (A,B,C…) warden mit dieser Option nicht mehr beachtet.
router2(config)#interface E0	Ethernet0 Schnittstelle auswählen.
router2(config-if)#ip address 10.0.5.254 255.255.254.0	IP-Adresse und Subnetzmaske für Ethernet0 definieren. Die weiteren Schnittstellen werden mit gleichem Vorgehen konfiguriert. Siehe Router-Config für Schnittstellen-Details.
router2(config-if)#no shut	Schnittstelle aktivieren.
router2(config)#exit	Config-Modus verlassen.
router2#write	Startup-Config wird mit Running-Config überschrieben.

E:\ÜK146\Routing\
Config Router2.txt

4.2.6 Aufgabe 6

A) Eine Routing-Table findet man in der Config des Routers.
→ Siehe Aufgabe 5 (Config-Files des entsprechenden Routers).
B) CLI-Befehl: „show ip route“.
C) Windows Befehl: „route print“.

4.2.7 Aufgabe 7

Folgende Tests bewiesen uns die Funktionsfähigkeit unseres Netzwerks und bestätigen somit die korrekte Konfiguration der beiden Router:

- Ping von LAN-C-Client „10.0.4.1“ an LAN-A-Client „10.0.0.1“
- Routenverfolgung mit tracert von LAN-C-Client zu LAN-A-Client.

4.2.8 Aufgabe 8

Diverse experimentelle Änderungen wurden am Testnetz vorgenommen.

4.2.9 Aufgabe 9

Kommando	Bemerkung
router1>enable	Mit “enable” in den Admin-Modus wechseln.
router1#config terminal	Konfiguration via Terminal vornehmen.
router1(config)#ip route 0.0.0.0 0.0.0.0 10.0.3.254	Default Gateway definieren, falls nicht bereits eingetragen.
router1(config)#router rip	Dynamisches Routing wird aktiviert.
router1(config-router)#network 10.0.0.0	Netzwerk definieren.
router1(config-router)#version 2	RIP Version 2 wählen.
router1(config-router)#exit	Config-Modus verlassen.
router1#write	Startup-Config wird mit Running-Config überschrieben.

4.2.10 Aufgabe 9

Kommando	Bemerkung
router1>enable	Mit “enable” in den Admin-Modus wechseln.
router1#config terminal	Konfiguration via Terminal vornehmen.
router1(config)#banner line	Banner-Befehl für die Eingabe
Enter TEXT message. End with character ’L’. ========== Cargo Steiner AG Internet Services ==========	