AKADEMIE FÜR LEHRERFORTBILDUNG UND PERSONALFÜHRUNG
DILLINGEN

SCHULNETZ

Qualifizierung von Beraterinnen
und Beratern digitale Bildung

Sichere Internetanbindung von Schulen

– Laborübungen –

Dillingen, September 2022

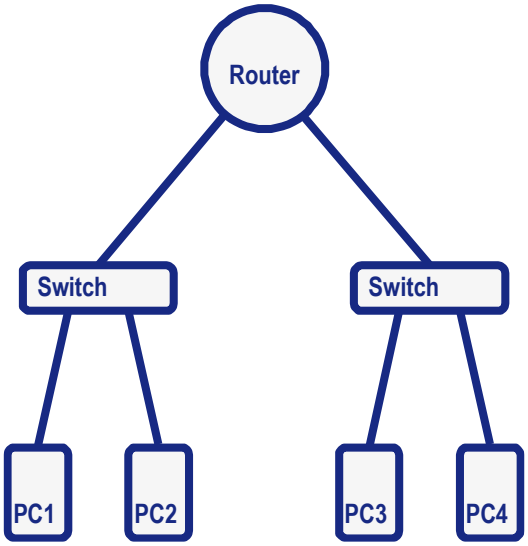
IMPRESSUM

Herausgeber:	Akademie für Lehrerfortbildung und Personalführung Kardinal-von-Waldburg-Str. 6-7 89407 Dillingen
Autoren:	Thomas Stallinger, Akademie Dillingen Markus Bader, Staatliche Berufsschule III, Fürth Barbara Maier
URL:	https://alp.dillingen.de/schulnetz
Mail:	stallinger@alp.dillingen.de
Stand:	September 2022

INHALT

LABORÜBUNG 01 - VERBINDUNG ZWEIER NETZE

Zwei Netze sollen über einen Router verbunden werden.



Aufgaben

1. Tragen Sie in den oben dargestellten logischen Netzplan die IP-Adressen und Subnetzmasken der PCs und des Routers ein.
2. Verbinden Sie die Netze entsprechend der obigen Darstellung und konfigurieren Sie die Computer und den Router, so dass eine Kommunikation zwischen allen Computern möglich ist.
3. Pingen Sie von einem Computer aus alle anderen Computer an und werten Sie anschließend die ARP-Tabelle aus. Interpretieren Sie die Einträge.
4. Notieren Sie die Routingtabelle des Routers und interpretieren Sie diese.

Zieladresse	Subnetzmaske	Gateway	Schnittstelle	Metrik

5. Notieren Sie die relevanten Einstellungen der Routingtabelle an einem Ihrer Computer und interpretieren Sie diese.

Zieladresse	Subnetzmaske	Gateway	Schnittstelle	Metrik

Umgang mit dem Router

6. Speichern Sie die Konfiguration des Routers ab. Setzen Sie den Router auf die Default-Einstellungen zurück und lesen Sie die Konfiguration wieder ein.

HINWEISE

`arp -a`	Ausgabe der ARP-Tabelle an einem Windows-PC
`route print`	Ausgabe der Routingtabelle an einem Windows-PC
`route -n`	Ausgabe der Routingtabelle an einem Linux-PC
`ipconfig`	Anzeige der lokalen IP-Einstellungen
`ipconfig /all`	Ausführliche Konfigurationsinformationen
`ipconfig /release`	Die aktuelle DHCP-Zuweisung für alle Netzwerk-Schnittstellen (Interfaces) wird freigegeben.
`ipconfig /renew`	Die DHCP-Zuweisung aller Netzwerk-Schnittstellen wird erneuert.

Notizen

APIPA-Adressen

Um auch ohne DHCP-Server mit dynamisch zugewiesenen IP-Adressen kommunizieren zu können, werden zufällig ausgewählte Adressen aus dem APIPA-Adressbereich 169.254.0.0/16 (Automatic Private IP Addressing) verwendet. APIPA-Adressen deuten darauf hin, dass der DHCP-Server nicht erreichbar ist.

Private IP-Adressen

Bestimmte IP-Adressen sind für die Nutzung innerhalb von LANs vorgesehen. Diese privaten IP-Adressen stehen weltweit allen Nutzern zur Verfügung. Da eine IP-Adresse immer eindeutig sein muss, werden diese Adressen nicht im Internet verwendet.

Privater Adressbereich	Standard-Subnetzmaske	Klasse (veraltet)
10.0.0.0 - 10.255.255.255	255.0.0.0	A
172.16.0.0 - 172.31.255.255	255.255.0.0	B
192.168.0.0 - 192.168.255.255	255.255.255.0	C

Multicast-Adressen

Um mehrere Computer gleichzeitig ansprechen zu können (z. B. bei Videoübertragungen oder beim Klonen mehrerer Computer), weisen diese Programme den beteiligten Computern zusätzlich eine Multicast-Adresse zu.

Adressbereich: 224.0.0.0 - 239.255.255.255

Loopback-Adressen

Mit einer Loopback-Adresse wird der eigene Computer angesprochen. Üblicherweise wird dazu die Adresse 127.0.0.1 verwendet.

Loopback-Adressen: 127.0.0.1 - 127.255.255.254

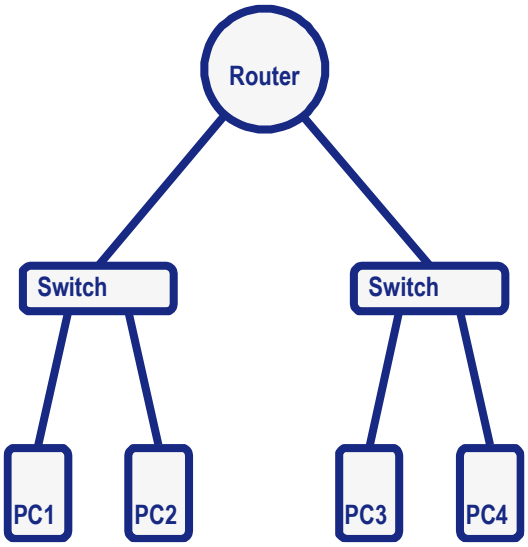
Broadcast Adressen

Die Kommunikation innerhalb eines Netzes erfordert auch Rundspruch-Nachrichten an alle Geräte. Broadcasts werden von Routern nicht an andere Netze weitergeleitet. Innerhalb eines Netzes spricht man deshalb von einer Broadcast-Domäne. Als Broadcast-Adresse ist immer die letzte IP-Adresse des Netzwerkadressbereiches definiert.

Broadcast-Adresse des Netzes 192.168.1.0/24: 192.168.1.255

Allgemeine Broadcast-Adresse: 255.255.255.255

Ergänzende Übung



Aufgaben

Beobachten Sie mit einem Netzwerksniffer[1] einen Ping von PC1 zu PC4. Notieren Sie die MAC- und IP-Adressierungen der einzelnen Ping-Pakete (Ethernet-Frames).

Ethernet-Frame von PC1 zum Router

Ziel-MAC	Quell-MAC	Quell-IP	Ziel-IP

Ethernet-Frame von Router zum PC4

Ziel-MAC	Quell-MAC	Quell-IP	Ziel-IP

Ethernet-Frame von PC4 zum Router

Ziel-MAC	Quell-MAC	Quell-IP	Ziel-IP

Ethernet-Frame von Router zum PC1

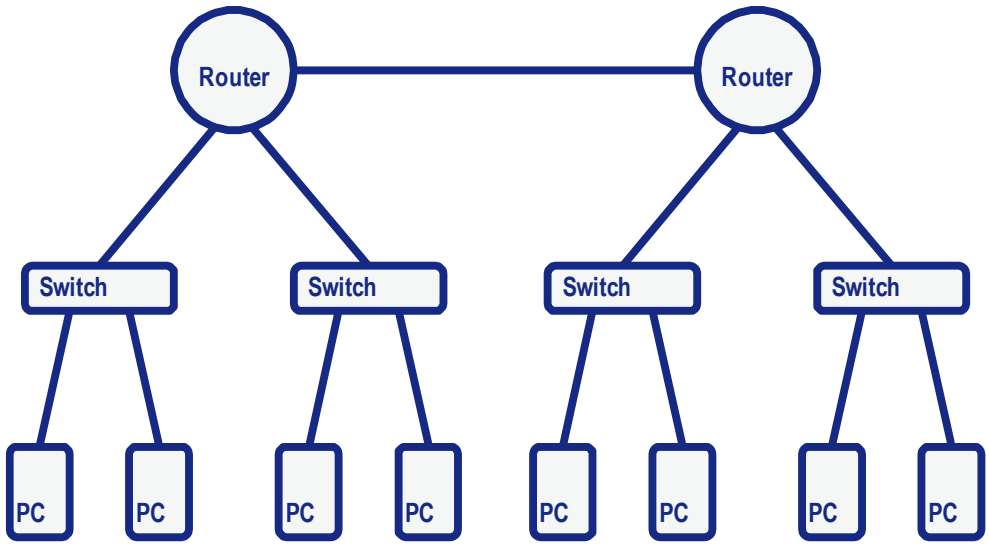
Ziel-MAC	Quell-MAC	Quell-IP	Ziel-IP

[1] siehe „Laborübung 11 - Analyse des Netzwerkverkehrs mit Wireshark“

Notizen

LABORÜBUNG 02 - ROUTING ZWISCHEN MEHREREN NETZEN

Mehrere Netze sollen über Router verbunden werden.



Aufgaben

1. Fertigen Sie in Ihrer Gruppe anhand der obigen Skizze einen logischen Netzplan an und notieren Sie in diesem Netzplan alle relevanten IP-Einstellungen. Einigen Sie sich in Ihrer Gruppe wer für welches Netz und für welchen Router verantwortlich ist.
2. Konfigurieren Sie die Computer und Router entsprechend Ihrem Verantwortungsbereich und überprüfen Sie die Kommunikation zwischen allen Geräten.
3. Notieren Sie die Routingtabelle Ihres Routers und interpretieren Sie diese.

Zieladresse	Subnetzmaske	Gateway	Schnittstelle	Metrik

HINWEISE

Statische Route

Eine statische Route ist ein festgelegter Weg zu einem bestimmten Netz. Eine statische Route wird vom Administrator manuell in die Routerkonfiguration eingetragen. In der Regel sind folgende Angaben notwendig:

- Zieladresse
- Subnetzmaske
- Gateway
- Schnittstelle
- Metrik

Default Route

Dies ist ein Sonderfall einer statischen Route und definiert einen festgelegten Weg für Datenpakete deren Zielnetze nicht explizit in der Routingtabelle stehen.

Dynamische Route

Die Routen werden durch Routingprotokolle festgelegt. Die Router informieren sich gegenseitig über ihre angeschlossenen Netze.

Direkte Route

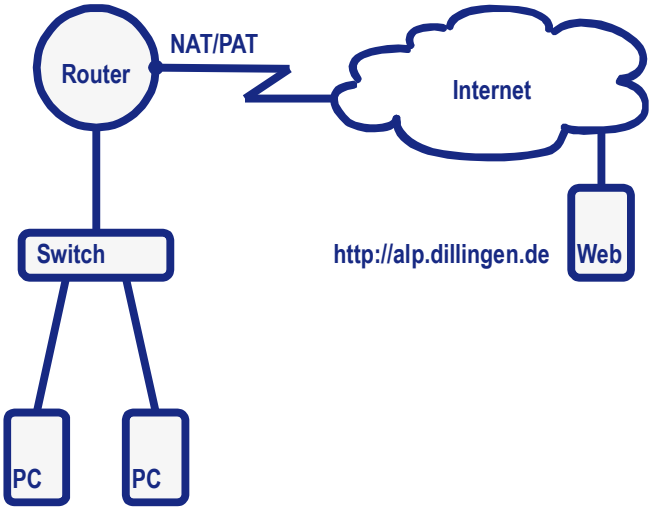
Eine Route in ein direkt am Router angeschlossenes Netz. Direkte Routen erkennt ein Router selbständig.

Indirekte Route

Eine Route in ein Netz, das nur über mindestens einen anderen Router erreichbar ist. Indirekte Routen müssen dem Router bekanntgegeben werden (als statische oder dynamische Routen). Der entfernte Router fungiert dabei als Gateway.

LABORÜBUNG 03 - ANBINDUNG AN DAS INTERNET

Ein lokales Netz soll an das Internet oder an das Hausnetz angeschlossen werden.



Aufgaben

1. Beschriften Sie im obigen Netzplan die PCs, die Schnittstellen des Routers und gegebenenfalls den Webserver mit IP–Adressen.
2. Verbinden Sie den Router mit dem Internet bzw. dem Hausnetz und testen Sie, in wie weit die Verbindung funktioniert.
3. Aktivieren Sie am externen Interface die NAT/PAT-Funktion.
4. Surfen Sie im Internet auf die ALP-Webseiten (https://www.alp.dillingen.de). Lesen Sie anschließend am Router die Netzadressübersetzungstabelle aus und ergänzen Sie die nachstehende NAT-Tabelle:

Proto-koll	Interne Adresse	Interner Port	Externe Adresse	Externer Port	Remote-Adresse	Remote Port

Weiterführende Aufgaben

5. Richten Sie den Router als DHCP-Server und DNS-Relay /-Proxy ein.
6. Begründen und zeigen Sie, dass aus dem Internet bzw. aus dem Hausnetz kein Zugriff auf Ihren Router oder auf Ihr internes LAN möglich ist, der nicht aus dem internen LAN initiiert wurde.

HINWEISE

`ipnattable`	Anzeige der NAT-Tabelle am Router über einen Konsolen-Zugang.
`SNMP-Browser`	Anzeige der NAT-Tabelle am Router über das Webinterface unter `ipnattable`

NAT – Network Address Translation (Netzadressübersetzung)

Damit ein Computer im lokalen Netz mit Computern im Internet kommunizieren kann, ersetzt der Router die Quelladressen aller IP-Pakete, die das lokale Netz verlassen, mit einer öffentlichen IP-Adresse (Netzadressübersetzung).

PAT – Port Address Translation (Portadressübersetzung)

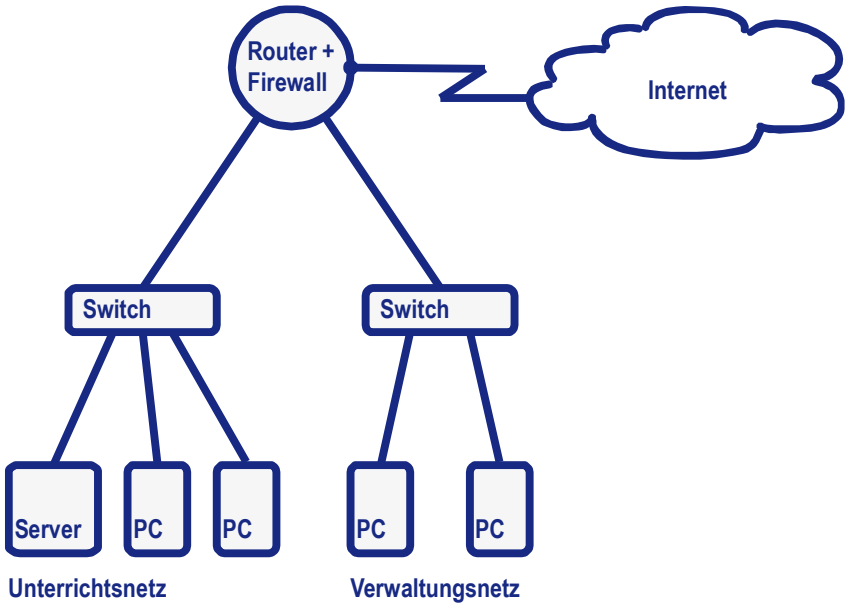
Bei PAT werden mehreren Computern mit privaten IP-Adressen eine oder mehrere öffentliche IP-Adressen zugewiesen. Durch die gemeinsame Nutzung einer öffentlichen IP-Adresse durch mehrere Computer werden zur Differenzierung der Kommunikationsstränge noch Portnummern herangezogen.

DNS-Relay / DNS-Proxy

Ist in einem Netz kein DNS-Server vorhanden, kann der Router als DNS-Relay bzw. DNS-Proxy eingerichtet werden. In der Client-Konfiguration wird der Router als DNS-Server eingetragen. Der Router nimmt die DNS-Anfragen der Clients entgegen und reicht diese an einen ihm bekannten DNS-Server weiter bzw. antwortet selber.

LABORÜBUNG 04 - EINRICHTEN EINER FIREWALL

Die Verwaltung der Schule und das pädagogische Netz sollen über denselben Zugangsrouter an das Internet angeschlossen werden. Der Informationsaustausch zwischen den beiden lokalen Netzen soll ausgeschlossen bzw. auf exakt festgelegte Szenarien beschränkt werden.



Aufgaben

1. Schließen Sie ein zweites lokales Netz (z. B. Verwaltungsnetz) an den Router an, so dass beide Netze einen Internetzugang haben.
2. Zeigen Sie, dass beide lokale Netze gegenseitigen Zugriff aufeinander haben.
3. Richten Sie eine Firewall ein und unterbinden Sie jede Kommunikation zwischen dem Verwaltungsnetz und dem Unterrichtsnetz. Der Zugriff in das Internet soll aus beiden Netzen heraus möglich sein.
4. Öffnen Sie die Firewall so, dass der Zugriff vom Verwaltungsnetz in das Unterrichtsnetz möglich ist. Der Zugriff in die umgekehrte Richtung soll weiterhin durch die Firewall geblockt werden.

Weiterführende Aufgabe

5. Beschränken Sie den Zugriff aus dem Verwaltungsnetz in das Unterrichtsnetz, so dass nur von einem Computer aus dem Verwaltungsnetz auf den Server im Unterrichtsnetz zugegriffen werden kann.
6. Beschränken Sie den Zugriff auf Ihren Router, so dass dieser nur von einem bestimmten Computer aus dem internen Netz konfigurierbar ist.

HINWEISE

Firewall Arten

Personal Firewall

Dabei handelt es sich um die auf dem Client lokal installierte Firewall. Sie soll unbefugte Zugriffe von außen auf Ressourcen des Clients unterbinden.

Externe Firewall

Sie befindet sich auf einem dezidierten Gerät, z. B. einem Router. Ihre Aufgabe ist nicht der Schutz des einzelnen Clients, sondern des Netzwerks.

Firewall-Techniken

Grundsicherung durch NAT

Nur Datenverkehr, der aus dem internen Netz initiiert wurde, ist möglich. Ein Verbindungsaufbau von außen scheitert an den nicht vorhandenen Einträgen in der NAT-Tabelle.

Packet-Filter

Die Filterung anhand von Access-Listen auf Layer 3 erfolgt, indem nach Quell- und Ziel-IP-Adresse gefiltert wird. Bei der Filterung auf Layer 4 werden zusätzlich noch die Portnummern berücksichtigt. Dadurch findet eine Service-Filterung statt. So kann beispielsweise nur http (Port 80) und https (Port 443) als zulässige Dienste im Internet definiert werden.

Stateful Inspection Firewall (SIF)

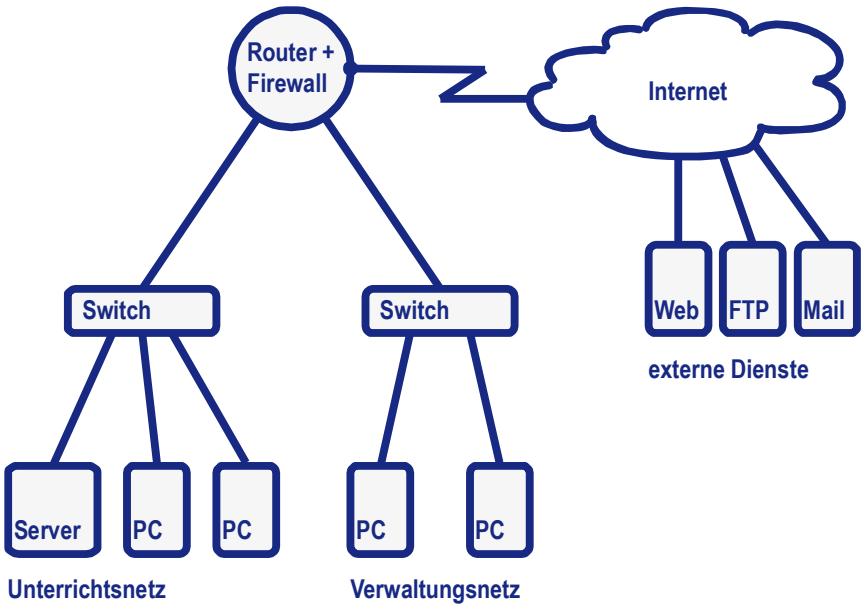
Die Stateful Inspection Firewall überprüft zusätzlich noch den Verbindungsstatus eines Datenpaketes.

Application Level Gateway (ALG)

Application Level Gateways ermöglichen eine Inhaltsfilterung der Datenpakete und arbeiten auf der Anwendungsschicht. Zusätzlich zu den Verkehrsdaten, wie Quelle, Ziel und Dienst, können hier noch die eigentlichen Nutzdaten (Payload) analysiert werden.

LABORÜBUNG 05 - BESCHRÄNKUNG DES INTERNETZUGANGS AUF EINZELNE DIENSTE

Der Zugang zum Internet soll nach den Vorstellungen der Schule abgesichert werden. Es sollen deshalb nur die Dienste möglich sein, die im jeweiligen Netz benötigt werden.



Aufgaben

1. Beschränken Sie die Zugriffe vom Unterrichts- und Verwaltungsnetz in das Internet auf die Dienste http und https.
2. Zur Pflege des Webservers der Schule soll zusätzlich aus beiden Netzen eine FTP-Verbindung zu diesem Webserver möglich sein. FTP-Verbindungen zu anderen Servern im Internet sind nicht erlaubt.
3. Ermöglichen Sie aus dem Verwaltungsnetz heraus die Nutzung von E-Mail (per SMTP und IMAP).
4. Ermöglichen Sie den Zugriff aus dem Verwaltungsnetz auf eine Freigabe auf dem Server im Unterrichtsnetz.

HINWEISE

Öffentlicher FTP-Server

ftp://ftp.adobe.com/pub

Testen eines Servers auf einen offenen Port mit der PowerShell

Die PowerShell lässt sich entweder über das Kontextmenü des  - Symbols öffnen oder durch die Eingabe des Begriffs im Suchfeld öffnen. Um auf einen offenen Port zu testen, verwendet man den Befehl Test-NetConnection <ip> -port <Nr>[2]. Es können auch Ports von Servern im Internet getestet werden.

Test-NetConnection ftp.adobe.com –Port 21

Test-NetConnection alp.dillingen.de –Port 80

Test-NetConnection 10.36.104.24 –Port 445

Test-NetConnection mail.gmx.net –Port 587

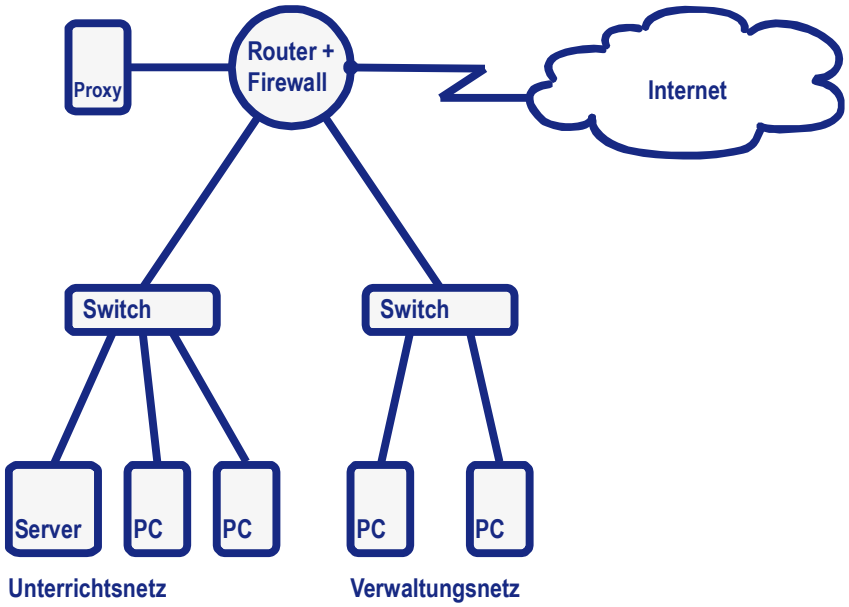
Test-NetConnection imap.gmx.net –Port 993

Notizen

[2] Eine Auswahl von wichtigen Ports finden Sie unter den Hinweisen im hinteren Bereich des Dokuments.

LABORÜBUNG 06 - WEB-ZUGRIFF ÜBER EINEN DNS-FILTER

Vom Unterrichtsnetz aus soll der Zugriff auf das Web nur über einen eingerichteten DNS mit Content-Filterung möglich sein.



Aufgaben

1. Testen Sie von einem PC aus den Webzugriff über den DNS und vergewissern Sie sich, dass beim Webzugriff über den DNS der eingerichtete Content-Filter wirkt.
2. Sorgen Sie dafür, dass der Webzugriff über http und https nur noch über den eingestellten DNS funktioniert. Sperren Sie dazu alle anderen Möglichkeiten, auf das Web zuzugreifen. Zudem soll eine manuelle Änderung des DNS-Servers am Client keine Auswirkungen haben.
3. Testen Sie die verschiedenen DNS-Server der ALP-Dillingen hinsichtlich der Filterstufen

Weiterführende Aufgaben

4. Das Verwaltungsnetz soll ohne Content-Filter in das Internet gehen können.

HINWEISE

Es gibt verschiedene Möglichkeiten einen Webfilter in ein Schulnetz technisch umzusetzen. Es kann zum einen eine Filterung über den DNS-Dienst, der von allen Geräten, die einen Internetzugang benötigen, eingesetzt werden. Eine externe DNS-Filterung bindet keine Ressourcen in der Schule, erlaubt jedoch keine differenzierten Filtereinstellungen innerhalb der Schule. Auf der anderen Seite gibt es die Möglichkeit einen Proxy im Schulnetz zu integrieren. Bei der Filterung von https-Seiten und bei der Arbeit mit mobilen Geräten bereiten Proxyserver häufig Probleme. Zahlreiche Apps bei Smartphones und Tablets funktionieren unter Verwendung eines Proxyservers nicht wie gewünscht.

Es besteht keine grundsätzliche Verpflichtung für Schulen, eine technische Lösung einzusetzen, um unerwünschte Internetseiten zu filtern bzw. Internetaktivitäten zu protokollieren.

DNS-Filter

Die Akademie bietet drei graduell verschieden eingestellte DNS-Server zu freien Nutzung durch Schulen an:

- Filterung von Malware: 194.95.207.171
- Filterung von Malware und pornografischen Seiten: 194.95.207.172
- Filterung von Malware, pornografischen Seiten und mehr: 194.95.207.173

Zudem gibt es die Möglichkeit den OpenDNS-Dienst (https://www.opendns.com) zu nutzen. Hier kann auch ein eigener Filter definiert werden.

Normaler Proxy

Im Internet-Browser wird der Proxy eingetragen. Alle Webanfragen werden an diesen Proxy gesendet.

Transparenter Proxy

Im Internetbrowser ist kein Proxy eingetragen. Durch eine Firewallregel werden Webanfragen an den Proxy umgeleitet.

Mögliche Funktionen eines Web-Proxy

- Zwischenspeicher von Webseiten
- Sicherheitsfunktion – Der externe Webserver erfährt nur die Adresse des Proxys
- Benutzerauthentifizierung
- Protokollierung der Webzugriffe nach Benutzernamen oder IP-Adresse (unter Beachtung des Datenschutzes nur möglich)
- Zeitgesteuerter Zugriff
- Webfilter (Z. B. URL-Filterlisten, Inhaltsfilter)
- Virenschutz

Grenzen eines Web-Proxy

Der Inhalt von https-Verbindungen kann nicht analysiert werden.

Ein transparenter Proxy funktioniert nicht in Verbindung mit einer Authentifizierung.

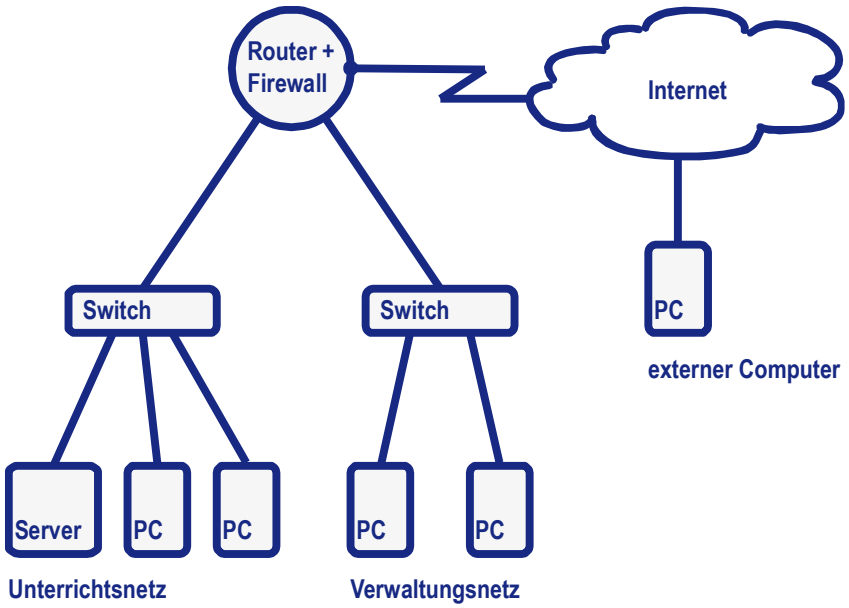
Ein transparenter Proxy funktioniert nicht in Verbindung mit einer https-Verbindung.

Openschoolproxy

https://www.openschoolproxy.de

LABORÜBUNG 07 - ZUGRIFF AUS DEM INTERNET AUF EINEN INTERNEN SERVER

Zur Remoteadministration soll auf einen internen Server zugegriffen werden.



Aufgaben

1. Richten Sie am Router das Portforwarding so ein, dass über das RDP-Protokoll (TCP-Port 3389) auf den Server im Schulnetz zugegriffen werden kann.
2. Verbinden Sie sich von einem PC außerhalb Ihres Netzes über eine RDP-Verbindung mit Ihrem Schulserver.
3. Ermöglichen Sie den RDP-Zugriff auf einen weiteren PC im LAN.
4. Ermöglichen Sie den RDP-Zugriff von außen bei aktivierter Firewall. Öffnen Sie die Firewall nur für die notwendigen Dienste.

HINWEISE

Port-Weiterleitung (Port Forwarding)

Um gezielt Verbindungen von außen zuzulassen (z. B. beim Betrieb eines öffentlich zugänglichen Webservers oder zur Fernadministration eines Servers), werden Zugriffe von außen auf bestimmte Ports der Zielrechner im internen Netz weitergeleitet.

Server, die von außen erreichbar sind, sind prinzipiell auch von außen angreifbar. Angriffe aus dem Internet erfolgen dabei üblicherweise, indem bekannt gewordene Sicherheitslücken der Serverdienste ausgenutzt werden oder durch ein automatisiertes Probieren von mehreren Tausend Benutzernamen- und Passwort-Kombinationen.

UPnP (Universal Plug and Play)

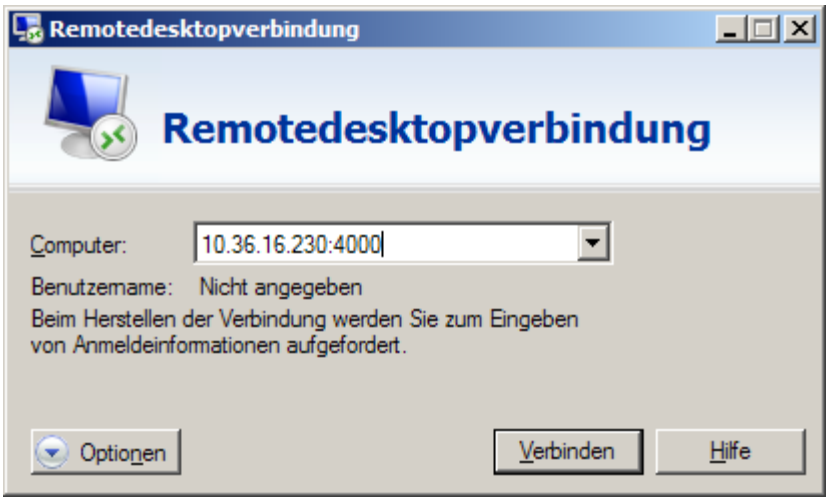
Die UPnP-Funktion eines Routers bietet einem Clientprogramm die Möglichkeit, die Konfiguration eines Routers nach den eigenen Erfordernissen anzupassen. Genutzt wird diese Funktionalität z. B. von Peer-to-Peer-Software (Tauschbörsen), die damit eine Port-Weiterleitung am Router einrichten.

Wer an seinem Router UPnP ermöglicht, braucht über das Thema Sicherheit nicht weiter nachzudenken.

Aufbau einer RDP-Verbindung (Port 3389)

Am Windows-Server: Remotedesktop zulassen

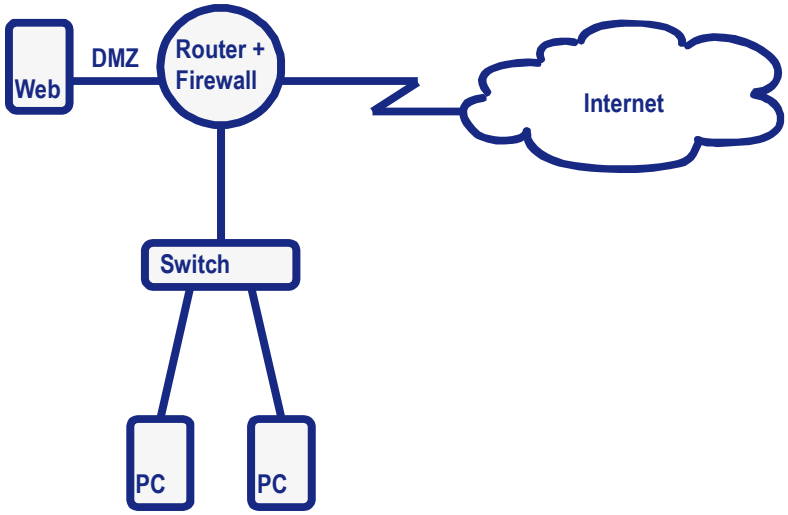
Am Windows-Client: Remotedesktopverbindung öffnen (mstsc.exe)



Aufruf einer RDP-Verbindung zu einem Windows-Server über einen alternativen Port.

LABORÜBUNG 08 - ZUGRIFF AUS DEM INTERNET AUF EINEN INTERNEN SERVER IN DER DMZ

Der Webserver der Schule soll aus dem Internet erreichbar sein.



Aufgabe

1. Richten Sie eine DMZ (Demilitarisierte Zone) ein und installieren Sie auf einem Ihrer PCs einen Webserver in der DMZ. Richten Sie den Router so ein, dass ein Zugriff vom Internet aus auf den Webserver auf Port 80 möglich ist.

HINWEISE

Miniwebserver

http://www.aidex.de

http://www.pablosoftwaresolutions.com

DMZ

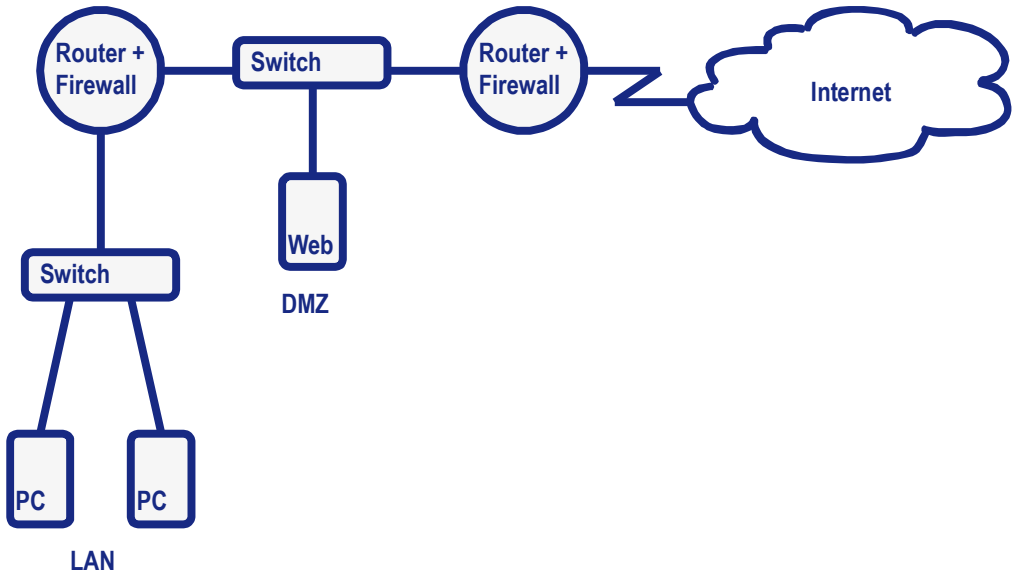
Eine DMZ ist ein vom übrigen LAN getrenntes Netz, in das Zugriffe von außen möglich sein sollen.

Einstufige Firewall / DMZ

Die DMZ wird an ein separates LAN-Interface angeschlossen. Die Firewallregeln werden so konfiguriert, dass ein Zugriff aus dem Internet nur in die DMZ möglich ist.

Zweistufige Firewall / DMZ

Das interne Netz ist durch einen separaten Router mit einer eigenen Firewall geschützt.



Beispiel für eine DMZ mit zweistufigem Firewallkonzept.

…

VPN-Verbindungen

VPN steht für „Virtual Private Network“ und meint damit eine virtuelle Verbindung zwischen zwei Computern oder Netzen über das Internet. Die Idee einer VPN-Verbindung ist es, dass z. B. ein Benutzer an seinem PC zu Hause Zugriff auf die Ressourcen am Arbeitsplatz hat.

Bei der VPN-Verbindung wird über das Internet eine verschlüsselte Verbindung (Tunnel) von einem VPN-Client zu einem VPN-Einwahlserver (VPN-Gateway) im Zielnetz aufgebaut. Dieser Einwahlserver muss über eine öffentliche IP-Adresse im Internet erreichbar sein.

Als Einwahlserver kann auch der Internetzugangsrouter dienen, falls dieser die Funktionalität unterstützt. Andernfalls werden am Internetzugangsrouter die entsprechenden Verbindungsanfragen zum VPN-Einwahlserver weitergeleitet (z. B. Port-Forwarding).

Die Verschlüsselung erfolgt immer zwischen den beiden VPN-Kommunikationspartnern.

Begrifflichkeiten

Authentisierung (engl. authentication):
Nachweis einer Identität, z.B. durch Benutzername und Passwort

Authentifizierung bzw. Authentifikation (engl. authentication):
Überprüfung der Identität eines Benutzers, z.B. durch Benutzername und Passwort

Autorisierung: Berechtigung, bestimmte Aktionen durchzuführen, z.B. auf Ressourcen im Netz zugreifen

Ziel einer VPN-Verbindung

Vertraulichkeit: Der Inhalt der Nachricht ist geheim.

Authentizität: Die Nachricht ist eindeutig vom angegebenen Absender.

Integrität: Der Inhalt der Nachricht wurde nicht verändert.

Site-to-End-VPN

Über einen VPN-Tunnel wird ein einzelner Computer in das Zielnetz eingebunden. Dieser Computer authentifiziert sich an einem Einwahlserver im Zielnetz und baut eine verschlüsselte Verbindung zu diesem Einwahlserver auf.

Site-to-Site-VPN

Über einen VPN-Tunnel werden zwei Netze verbunden. Der Internetzugangsrouter in einem Filialnetz verbindet sich mit dem Einwahlserver im Unternehmensnetz. Die verschlüsselte Verbindung wird zwischen dem Internetzugangsrouter und dem Einwahlserver aufgebaut.

Site-to-Site-VPN-Verbindungen werden mitunter auch bereits vorkonfiguriert zwischen baugleichen Internetzugangsroutern angeboten.

End-to-End-VPN

Über einen VPN-Tunnel werden zwei Computer miteinander verbunden. Die verschlüsselte Verbindung wird zwischen den beiden Computern aufgebaut.

Eine Variante von End-to-End VPN-Verbindungen stellen auch externe Dienste, wie z. B. Hamachi oder Team-Viewer an, bei denen sich zwei Computer über einen vermittelnden Server im Internet verbinden.

VPN-Protokolle

PPTP	Point to Point Tunneling Protocol (Layer 2)
L2TP	Layer 2 Forwarding (Layer 2)
IPSec	IP Security Protocol (Layer 3)
TLS/SSL	Transport Layer Security / Secure Sockets Layer (Layer 4-7), z. B. OpenVPN, SSL-Explorer

Proprietäre Protokolle (z. B. Hamachi, Team-Viewer)

PPTP

Das PPTP-Protokoll ist in den Microsoft-Betriebssystemen bereits implementiert. Deshalb benötigt ein Windows-Client keine Zusatzsoftware, um sich mit einem PPTP-Einwahlknoten zu verbinden. Leider gelten die eingesetzten Verschlüsselungs- und Authentifizierungsverfahren seit langem als gebrochen und somit unsicher an.

Der Verbindungsaufbau bei PPTP erfolgt über TCP Port 1723. Die verschlüsselten Daten werden über das GRE-Protokoll (Generic Routing Encapsulation) übertragen.

IPSec

IPSec arbeitet auf der Schicht 3 des ISO/OSI-Modells. Die originalen IP-Pakete werden bei einer Site-to-Site-Verbindung (sog. Tunnelmodus) verschlüsselt und in weitere IP-Pakete verpackt. Es ist auch im neuen IPv6 Standard integriert.

Teilprotokolle von IPSec

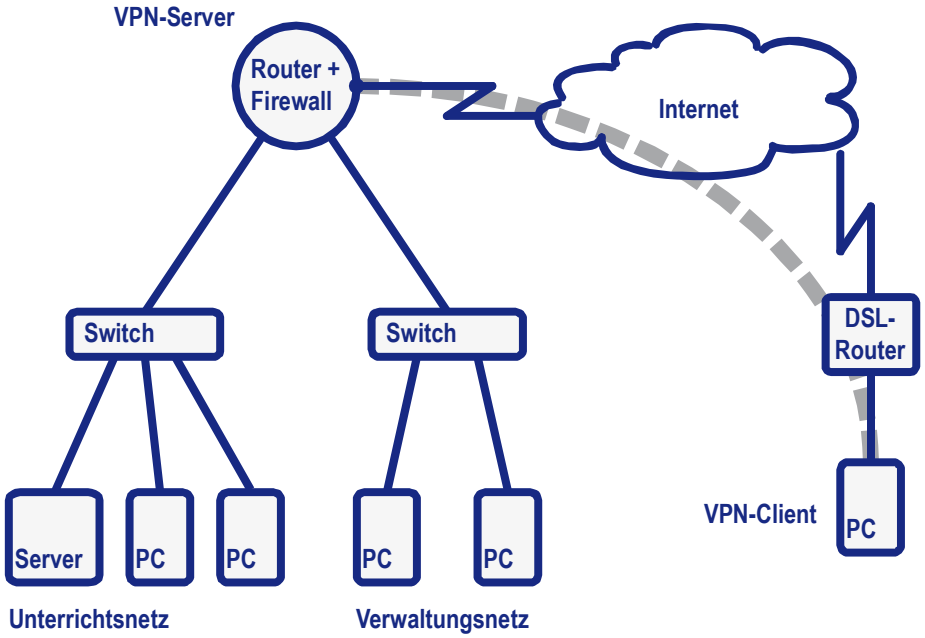
AH - Authentication Header

ESP - Encapsulation Security Payload

IKE - Internet Key Exchange

LABORÜBUNG 09 - VPN-VERBINDUNG IN DAS SCHULNETZ (IPSEC)

Von zu Hause aus soll eine gesicherte VPN-Verbindung (über das IPSec-Protokoll) in das Schulnetz eingerichtet werden (User-to-Site-VPN).



Aufgaben

1. Richten Sie (mit Hilfe des Assistenten) den Router als IPSec-VPN-Server ein. Die Clients sollen bei der Verbindung eine IP-Adresse aus dem Unterrichtsnetz erhalten.
2. Stellen Sie von einem externen Client eine VPN-Verbindung her und überprüfen Sie, auf welche internen Netze und PCs Sie zugreifen können.
3. Beweisen Sie, dass die Datenübertragung verschlüsselt ist.
4. Überprüfen Sie, auf welchem Weg der externe Client eine beliebige Internetverbindung aufbaut.

Weiterführende Aufgabe

5. Konfigurieren Sie den Router auf Basis der durch den Assistenten gesetzten Werte manuell.

HINWEISE

IPSec-Clients

Die Firma bintec elmeg bietet für ihre Router eigene IPSec-Clients an, mit denen die Konfiguration über einen Assistenten sehr einfach ist.

Eine zeitlich limitierte Testversion kann heruntergeladen werden (Suchbegriffe: bintec ipsec client).

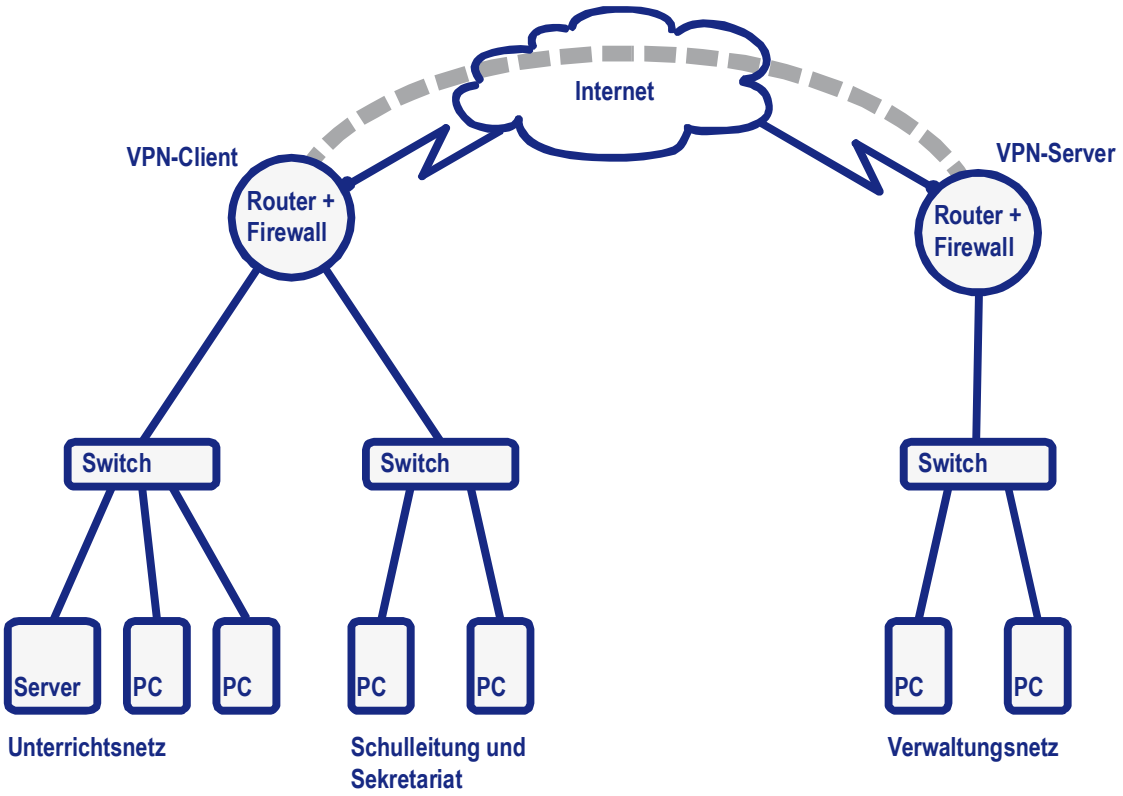
Für IPSec stehen auch kostenlose (Open Source) Clients zur Verfügung. Da IPSec sehr viele Konfigurationsoptionen bietet, die auf der Client- und Serverseite genau zusammen passen müssen, ist es nicht einfach, diese Clients zu konfigurieren (erfolgreiche bisherige Tests: Shrew Soft VPN Client).

Notizen

LABORÜBUNG 10 - IPSEC-VPN ZWISCHEN ZWEI NETZEN

Schulleitung und Sekretariat einer Schule sollen über eine VPN-Verbindung an ein zentrales Verwaltungsnetz angeschlossen werden. Das Verwaltungsnetz befindet sich an einem anderen Standort und ist über das Internet erreichbar.

Mit IPSec soll eine Site-to-Site-Verbindung zwischen dem Router der Schule und dem Router der Verwaltung hergestellt werden.



Aufgaben

1. Richten Sie eine Grundkonfiguration der beiden Netze ein. Verzichten Sie zunächst auf Restriktionen durch eine Firewall. Beide Netze sollen Zugang zum Internet haben.
2. Richten Sie eine IPSec-Verbindung zwischen den beiden Routern ein. Nutzen Sie dazu die Konfigurationshinweise bzw. nutzen Sie den Konfigurationsassistenten. Schulleitung und Sekretariat sollen anschließend Zugriff auf das Verwaltungsnetz haben.

HINWEISE

IPSec-Modi

Transportmodus: Host to Host

Tunnelmodus: Site to Site

Konfiguration einer Site-to-Site-VPN unter IPSec mit PSK auf Bintec-Routern

Nach der Grundkonfiguration (Schnittstellen, IP-Adressen, Datum/Zeit) wird die eigentliche IPSec-VPN-Verbindung eingerichtet. Diese besteht aus drei Schritten:

1. Verbindung zur Gegenstelle (IPSec-Peers)
2. Phase-1: Schlüsselaustausch
3. Phase-2: Datenübertragung

Grundkonfiguration

Router der Schule

Unterrichtsnetz:	192.168.1.0 /24
Gateway:	192.168.1.254
Schulleitung und Sekretariat:	192.168.0.0 /24
Gateway:	192.168.0.254
Externe Schnittstelle:	10.10.10.1 /24 (NAT)

Router der Verwaltung

Verwaltungsnetz:	192.168.100.0 /24
Gateway:	192.168.100.254
Externe Schnittstelle:	10.10.10.2 /24 (NAT)

Die IP-Adressen der externen Schnittstellen müssen an die Laborumgebung angepasst werden.

Datum und Uhrzeit müssen auf beiden Routern übereinstimmen.

IPSec-Konfiguration

Verbindung zur Gegenstelle (IPSec-Peers)

Bintec-Menü: VPN → IPSec → IPSec-Peers → Neu

	Router der Schule	**Router der Verwaltung**
Administrativer Status	aktiv	aktiv
Beschreibung	Verbindung zur Verwaltung	Verbindung zur Schule
Peer-Adresse	10.10.10.2	10.10.10.1
Peer-ID – FQDN:	Verwaltung	Schule
Preshared Key	geheim	geheim
IP-Adressenvergabe	statisch	statisch
Standardroute	nicht markiert	nicht markiert
Lokale IP-Adresse	192.168.0.254	192.168.100.254
Routeneinträge	192.168.100.0/255.255.255.0	192.168.0.0/255.255.255.0
Erweiterte Einstellungen		
Startmodus	Immer aktiv	Auf Anforderung
Phase-1-Profile	** Profilname aus Phase 1*	** Profilname aus Phase 1*
Phase-2-Profile	** Profilname aus Phase 2*	** Profilname aus Phase 2*

* nach Konfiguration der Phase-1- und -2-Profile werden die Profile hier eingetragen

Bei allen weiteren Einstellungen kann die Vorgabe belassen werden.

Phase-1: Schlüsselaustausch

Bintec-Menü: VPN → IPSec → Phase-1-Profile → Neu / Phase-1-Parameter (IKE)

	Router der Schule	**Router der Verwaltung**
Beschreibung	*Profilname*	*Profilname*
Proposals	AES-256 / MD5	AES-256 / MD5
DH-Gruppe	2 (1024 Bit)	2 (1024 Bit)
Lebensdauer	14400 Sekunden	14400 Sekunden
Authentifizierungsmethode	Preshared Keys	Preshared Keys
Modus	Aggressiv	Aggressiv
Lokaler ID-Typ	Full Qualified Domain Name	Full Qualified Domain Name
Lokaler ID-Wert	Schule	Verwaltung
Erweiterte Einstellungen		
NAT-Transversal	aktiv	aktiv

Bei allen weiteren Einstellungen kann die Vorgabe belassen werden.

Phase-2: Datenübertragung

Bintec-Menü: VPN →IPSec → Phase-2-Profile → Neu / Phase-2-Parameter (IPSEC)

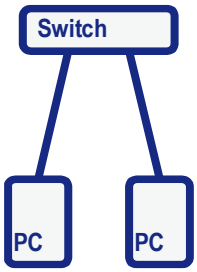
	Router der Schule	**Router der Verwaltung**
Beschreibung	*Profilname*	*Profilname*
Proposals	AES-256 / MD5	AES-256 / MD5
PFS-Gruppe verwenden	☑ Aktiviert / 2 (1024 Bit)	☑ Aktiviert / 2 (1024 Bit)
Lebensdauer	14400 Sekunden	14400 Sekunden

Bei allen erweiterten Einstellungen kann die Vorgabe belassen werden.

Notizen

LABORÜBUNG 11 - ANALYSE DES NETZWERKVERKEHRS MIT WIRESHARK

Zwei Computer sind über einen Switch verbunden. Der Netzwerkverkehr zwischen diesen beiden Computern soll protokolliert und analysiert werden. Um Nebeneffekte zu vermeiden, befinden sich keine weiteren Computer in diesem Netz.



Aufgaben

1. Vergeben Sie statische IP-Adressen aus dem Bereich 192.168.0.0/24 und überprüfen Sie die Verbindung der beiden Computer auf IP-Ebene.
2. Richten Sie an einem der beiden Computer eine Freigabe ein und tauschen Sie über diese Freigabe Dokumente aus.
3. Analysieren Sie mit Hilfe des Netzwerksniffers Wireshark die folgenden Vorgänge im Netz:
   - ARP-Anfrage
   - Ping
   - Namensauflösung
   - SMB-Zugriff

Notizen

HINWEISE

`arp -a`	Anzeige der ARP-Tabelle
`arp -d`	Löschen der ARP-Tabelle

Protokolle

Unter Windows: C:\Windows\System32\drivers\etc\protocol

Unter Linux: /etc/protocols

Ports/Portnummern

Unter Windows: C:\Windows\System32\drivers\etc\services

Unter Linux: /etc/services

http://www.iana.org/assignments/port-numbers

Wireshark

http://www.wireshark.org

Portadressen und damit verbundene Anwendungen

```
ftp-data        20/tcp      #FTP, data
ftp             21/tcp      #FTP, control
ssh             22/tcp      #Secure Shell
telnet          23/tcp      #Telnet
smtp            25/tcp      #Simple Mail Transfer Protocol
dns             53/tcp      #Domain Name Server
dns             53/udp      #Domain Name Server
dhcp            67/udp      #DHCP-Server oder Relay Agent
dhcp            68/udp      #DHCP-Client
http            80/tcp      #World Wide Web
pop3           110/tcp      #Post Office Protocol - Version 3
netbios-ns     137/tcp      #NETBIOS Name Service
netbios-ns     137/udp      #NETBIOS Name Service
netbios-dgm    138/udp      #NETBIOS Datagram Service
netbios-ssn    139/tcp      #NETBIOS Session Service
imap           143/tcp      #Internet Message Access Protocol
https          443/tcp      #http protocol over TLS/SSL
microsoft-ds   445/tcp      #Microsoft-Ds Active Directory, Windows Shares
microsoft-ds   445/udp      #Microsoft-DS, SMB file sharing
wins          1512/udp      #Microsoft Windows Internet Name Service
pptp          1723/tcp      #Point-to-point tunnelling protocol
```

Fragen zu Aufgabe 3

ARP-Anfrage

Ziel-Mac-Adresse: _____

Quell-Mac-Adresse: _____

Welche Information wird angefragt? _____

ARP-Antwort

Ziel-Mac-Adresse: _____

Quell-Mac-Adresse: _____

Wie lautet die angefragte Information? _____

ICMP-Anfrage

In welches Protokoll ist das ICMP-Paket eingebettet? _____

IP-Pakete

Ein eingehendes IP-Paket wird von einer Progammroutine verarbeitet. Woran erkennt das Programm, welches Protokoll (z. B. TCP, UDP, ICMP) im Datenteil (Payload) des IP-Pakets enthalten ist?

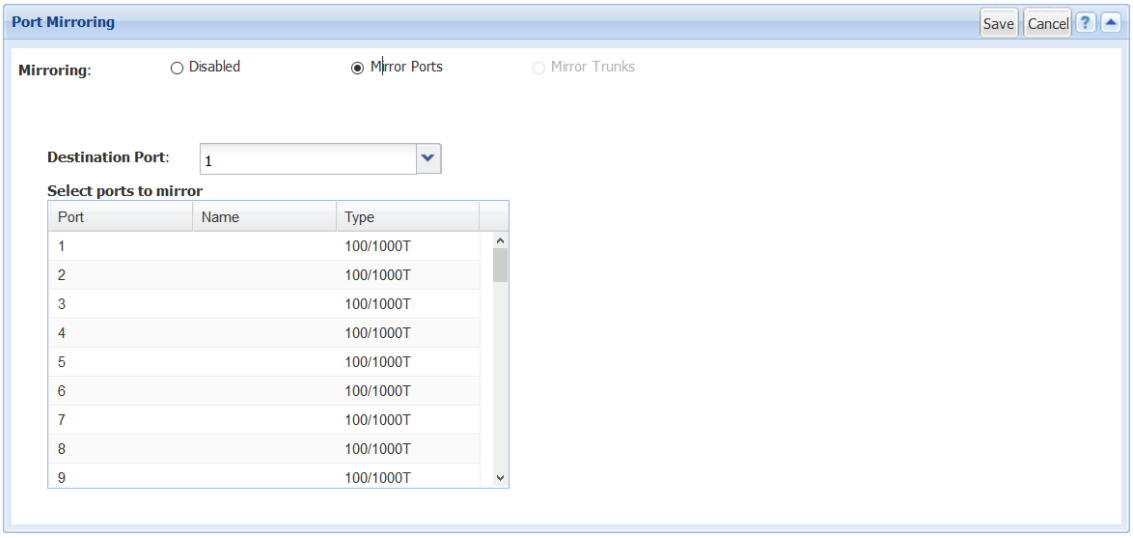
_____

Portnummern

Welchen Port verwendet die NetBIOS Namensauflösung? _____

Welche Ports werden für Windows-Freigaben verwendet? _____

Einrichten eines Monitoring-Ports an einem managebaren Switch



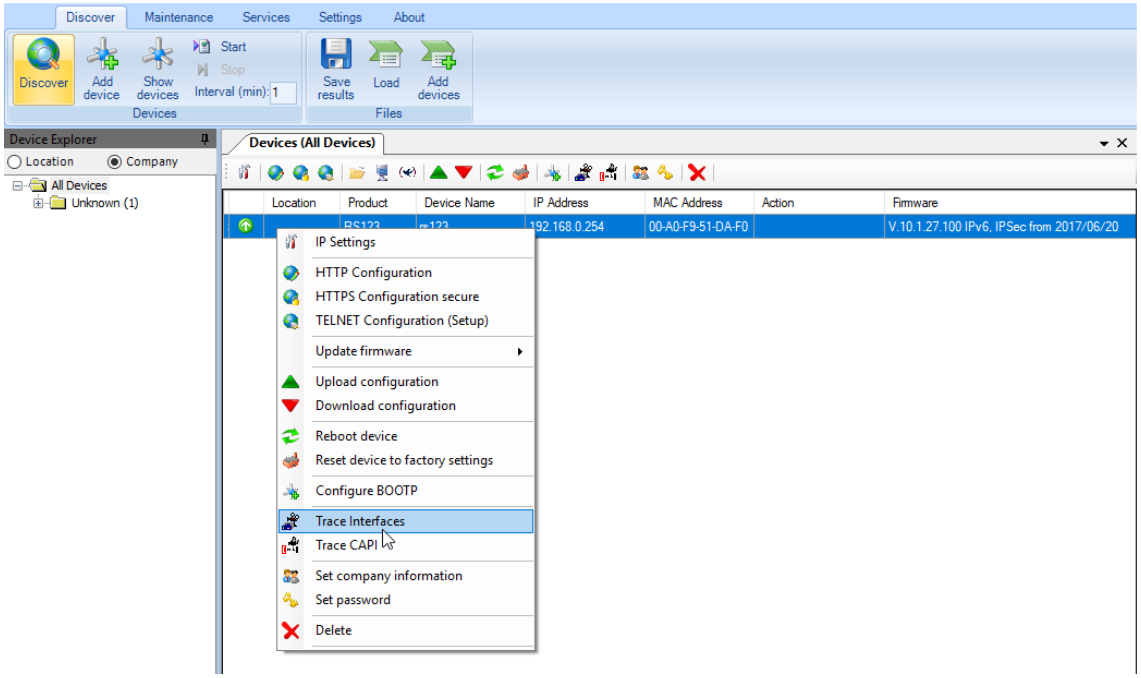
An vielen managebaren Switchen lässt sich ein Monitoring-Port einrichten, über deneinzelne Ports oder der gesamte Netzwerkverkehr am Switch gespiegelt werden. Dieser Monitoring-Port kann z. B. mit Wireshark abgehört werden, um Netzwerkprobleme zu lokalisieren.

LABORÜBUNG 12 - ANALYSE DES NETZWERKVERKEHRS AUF EINEM BINTEC-ROUTER

Über den Bintec DIME Manager kann der Datenverkehr an den Schnittstellen des Routers mitverfolgt und aufgezeichnet werden. Die aufgezeichneten Daten können mit dem Programm Wireshark analysiert werden.

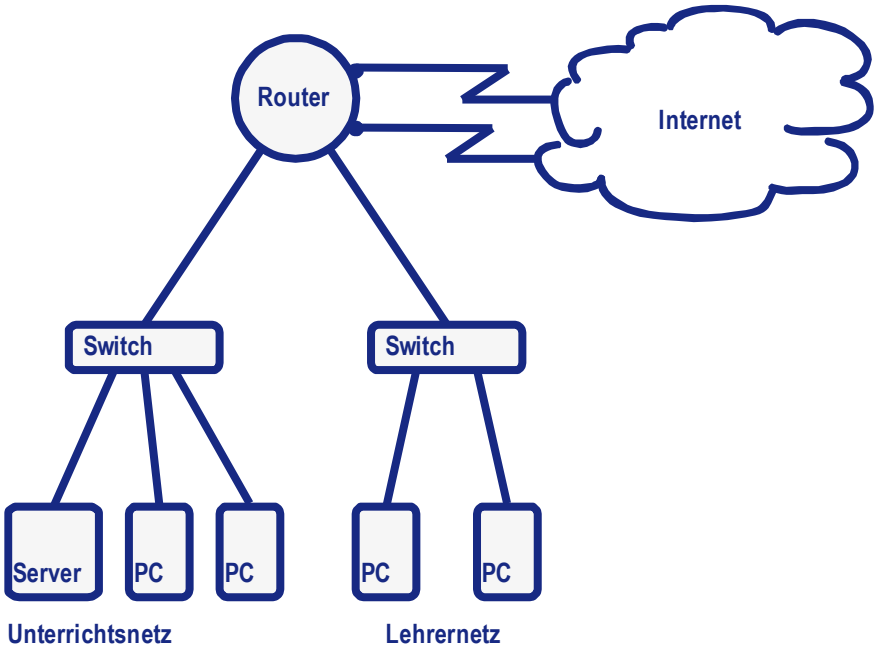
Hinweis: Der Bintec DIME Manager benötigt .NET Framework 3.5.

Nach der Authentifizierung am Router kann der Datenverkehr aufgezeichnet (Pcap – Save to File) und mit Wireshark analysiert werden.



LABORÜBUNG 13 - OPTIONAL: REDUNDANTE ANBINDUNG AN DAS INTERNET

Das lokale Netz soll über zwei redundante Internetanbindungen verfügen.



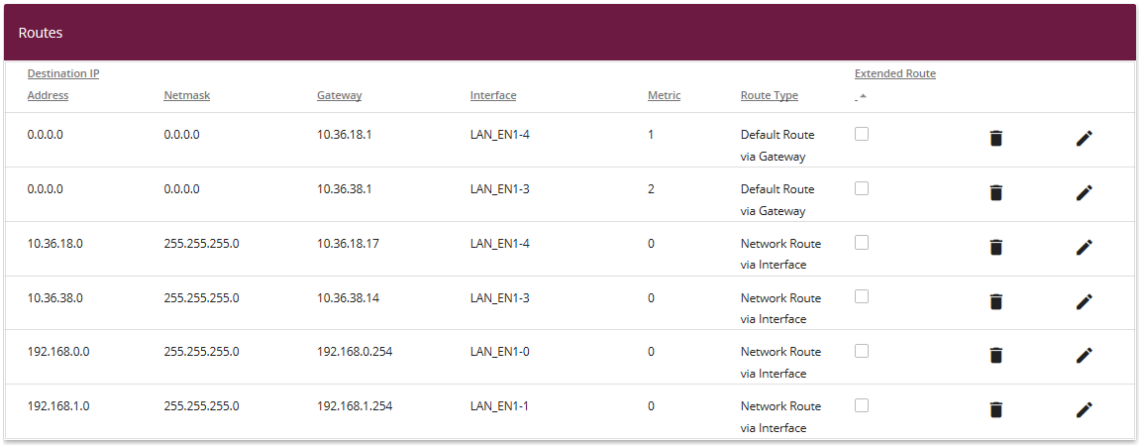
Voraussetzung

Es sind zwei unterschiedliche Anbindungen an das Hausnetz bzw. an das Internet notwendig.

Aufgaben

1. Richten Sie die beiden unterschiedlichen Anbindungen in das Hausnetz bzw. in das Internet ein. Testen Sie die beiden Verbindungen, indem Sie die Verbindungen wahlweise unterbrechen.
2. Richten Sie die Verbindungen so ein, dass eine Leitung als primäre Leitung verwendet wird und die zweite Leitung nur als Ausfallsicherheit dient.
3. Richten Sie zwischen den beiden Internetanbindungen ein Load-Balancing ein.
4. Konfigurieren Sie das Netz so, dass das Unterrichtsnetz und das Lehrernetz standardmäßig unterschiedliche Internetanbindungen nutzen. Wenn eine der beiden Leitungen ausfällt, soll automatisch die andere verwendet werden.

Mehrere Default-Routen



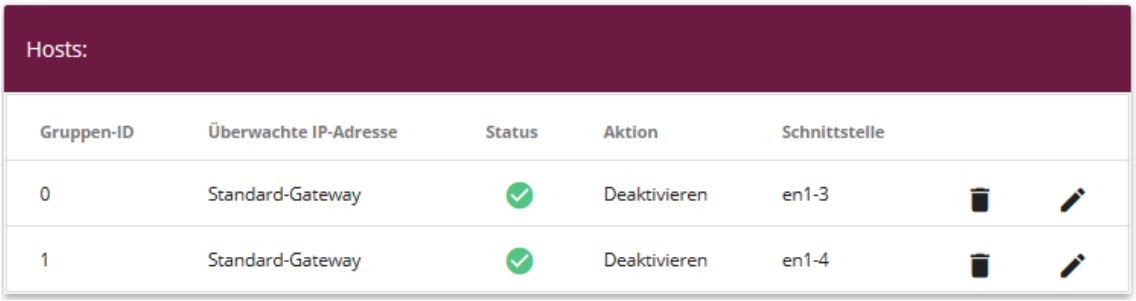
Routes

Destination IP Address	Netmask	Gateway	Interface	Metric	Route Type	Extended Route
0.0.0.0	0.0.0.0	10.36.18.1	LAN_EN1-4	1	Default Route via Gateway	
0.0.0.0	0.0.0.0	10.36.38.1	LAN_EN1-3	2	Default Route via Gateway	
10.36.18.0	255.255.255.0	10.36.18.17	LAN_EN1-4	0	Network Route via Interface	
10.36.38.0	255.255.255.0	10.36.38.14	LAN_EN1-3	0	Network Route via Interface	
192.168.0.0	255.255.255.0	192.168.0.254	LAN_EN1-0	0	Network Route via Interface	
192.168.1.0	255.255.255.0	192.168.1.254	LAN_EN1-1	0	Network Route via Interface	

Destination IP Address	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	10.36.18.1	LAN_EN1-4	1
0.0.0.0	0.0.0.0	10.36.38.1	LAN_EN1-3	2

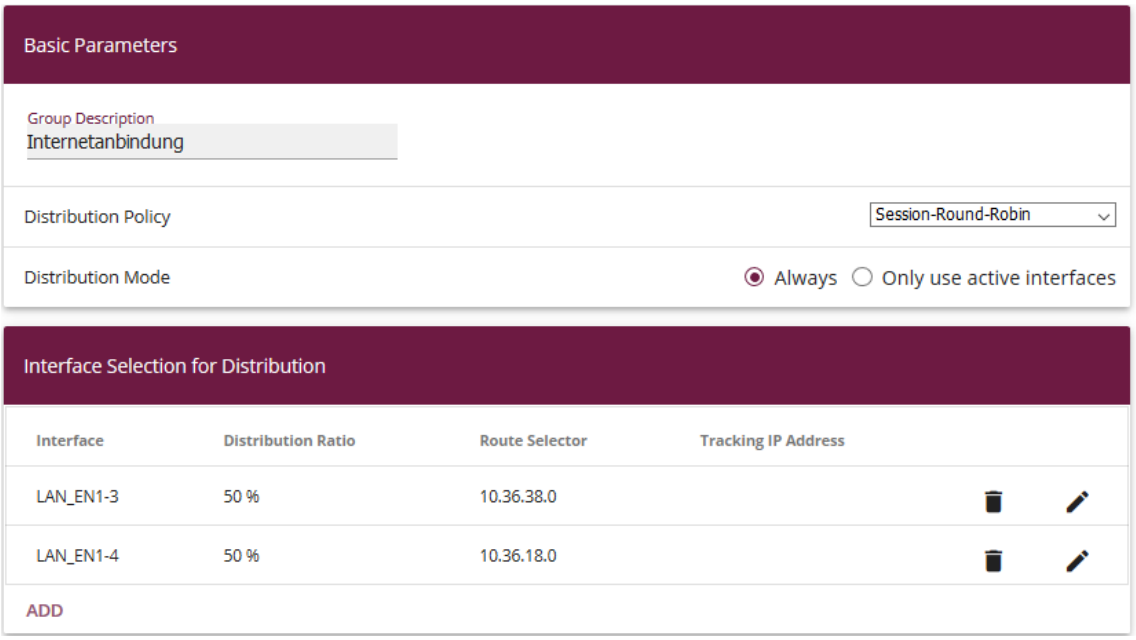
In der Routing-Tabelle sind zwei Default-Routen zu unterschiedlichen Gateways mit unterschiedlichen Metriken eingetragen. Wenn die primäre Leitung (Metrik 1) ausfällt, wird der Netzwerkverkehr über die zweite Verbindung geleitet.

Überwachung des Netzwerk-Verkehrs



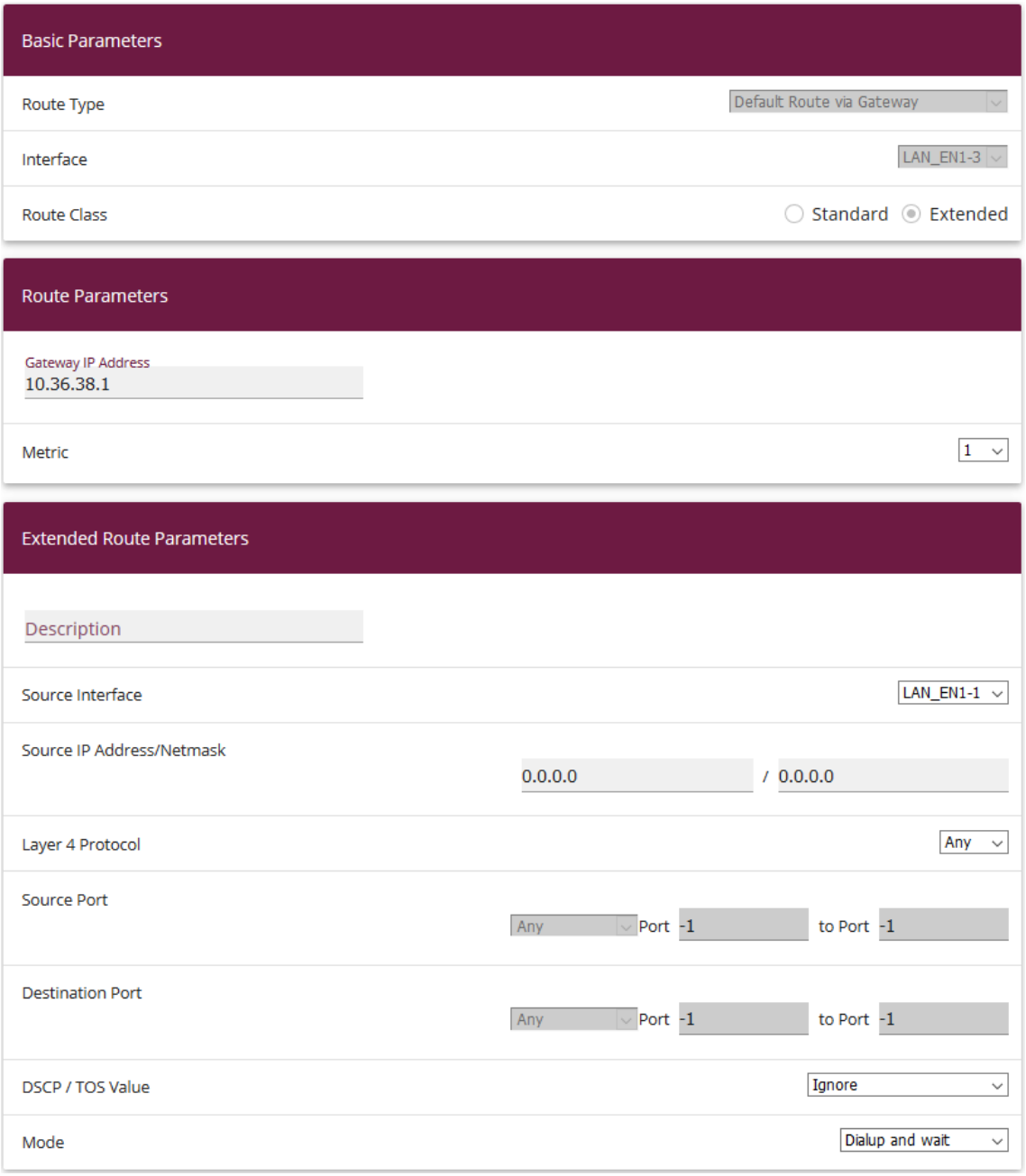
Wenn bei einer redundanten Anbindung die Verbindung nicht direkt am Router unterbrochen wird, wird diese Unterbrechung gegebenenfalls nicht erkannt. Der Router versucht weiterhin über die nicht funktionierende Verbindung zu senden. Um dies zu verhindern, kann die Verbindung über eine Route (bis zum Standard-Gateway oder bis zu einem entfernten Server) überwacht werden und die Schnittstelle bei Bedarf deaktiviert werden.

Load Balancing



Beim Load-Balancing wird der anfallende Netzwerkverkehr zwischen den vorhandenen Internetverbindungen aufgeteilt.

Erweiterte Routen

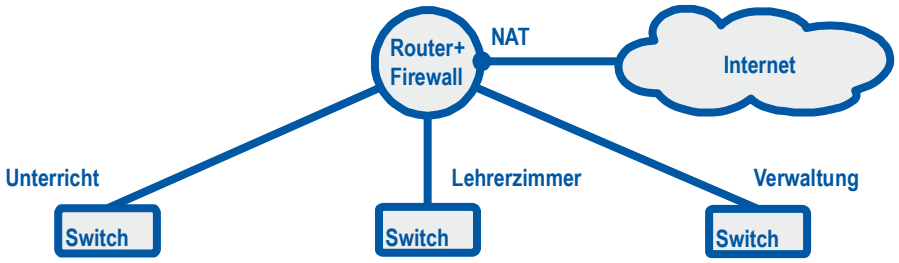


Während sich Standard-Routen nur an der Zieladresse orientieren, ist es bei erweiterten Routen auch möglich, Routing-Entscheidungen anhand der Absende Adresse oder anhand der Anwendung zu treffen.

LABORÜBUNG 14 - OPTIONAL: PLANUNG EINER SCHULSTRUKTUR

Eine Schule soll mit drei Netzen (Unterrichtsnetz, Lehrerzimmer, Verwaltung) und einem gemeinsamen Internetzugang eingerichtet werden

Logischer Netzplan



Aufgaben

1. Ergänzen Sie den logischen Netzplan mit den Computern und den notwendigen zentralen Geräten (z.B. Fileserver, Drucker).
2. Legen Sie fest, wer auf welche Geräte/Netzwerkbereiche zugreifen darf und skizzieren Sie entsprechende Firewall-Regeln.

HINWEISE

Beispiele für die Darstellung von Firewallregeln

von \ nach	Unterrichts-netz	Lehrerzimmer	Verwaltung	Internet
Unterrichts-netz		Kein Zugriff	Kein Zugriff	Zugriff auf We-binhalte über DNS-Filter
Lehrerzimmer				alle Ports
Verwaltung				

Quelle	Ziel	Dienste
Proxy Unterricht	Internet	Port 80,443
Lehrerzimmer	Internet	alle Ports

UMGANG MIT EINEM BINTEC-ROUTER

Konfigurationszugang

Die Konfiguration eines Routers kann über verschiedene Zugriffsmöglichkeiten erfolgen:

- Webinterface (http oder https)
- Telnet oder SSH
- SNMP (Simple Network Management Protocol)
- Konsole (serielle Schnittstelle; Terminal-Emulator)

Konsolenverbindung

Eine Konsolenverbindung hat den Vorteil, dass sie unabhängig von Netzwerkeinstellungen funktioniert. Diese Möglichkeit bieten in der Regel nur professionelle Router.

Zur Kommunikation dienen Terminal-Emulatoren z. B.:

- Hyper Terminal
- Putty
- Tera Term

Damit ein Computer und ein Router miteinander über die serielle Schnittstelle kommunizieren können, müssen die Übertragungsparameter beider Geräte übereinstimmen.

Bits pro Sekunde (Baudrate)	115200
Datenbits	8
Parität	Keine
Stoppbits	1
Flusssteuerung	Keine

Die Baudrate (Speed) beschreibt die Geschwindigkeit der Übertragung.

Durch die Angabe der Datenbits wird festgelegt, wie viele Bits pro Zeichen übertragen werden.

Das Paritätsbit dient zur Erkennung von Fehlern bei der Datenübertagung.

Das Stoppbit legt fest, wie lange nach dem Senden eines Zeichens gewartet werden soll, bis das nächste Zeichen übertragen wird.

Durch die Flusssteuerung stimmen sich die zwei Geräte ab, ob der jeweils andere gerade bereit zum Datenempfang ist oder nicht.

Standardzugangsdaten im Auslieferungszustand

```
Login:              admin
Password:           admin
```

Zurücksetzen des Bintec-Routers in den Auslieferungszustand

Nach dem Starten des Routers muss der Bootvorgang, durch betätigen der Leertaste (Space-Taste) unterbrochen werden:

```
Press <sp> for boot monitor or any other key to boot system
```

Danach erscheint ein Auswahlmenü:

```
(1) Boot System
…
(4) Delete Configuration
```

Ausgewählte Kommandozeilenbefehle

halt	Neustart
setup	Halbgrafische Bedienoberfläche
netstat –i	Anzeige der Interfaces
netstat –r	Routingtabelle
cmd=save	Speichern der Konfiguration
ipNatTable	Anzeigen der NAT-Tabelle
t 0	Timeout (autologout) abschalten
nslookup	DNS-Namensauflösung
ping	Diagnosewerkzeug auf IP-Ebene
telnet	Aufruf von Telnet
ifconfig –h	Zeigt alle Parameter zum Befehl ifconfig an
debug all &	Das & lässt eine weitere Eingabe zu.
exit	Abmelden
?	Hilfe

Web-Zugriff

Die Konfiguration des Routers erfolgt in der Regel über die Web-Oberfläche. Nach dem Zurücksetzen des Routers bzw. in der Standardkonfiguration ist der Router auf der interne Schnittstelle (en1-0, Port 1-4) unter der IP-Adresse 192.168.0.254 erreichbar.

```
Login:                  admin
Password:               admin
```